Санкт-Петербургский государственный университет

**АЛЕКСЕЕВ Ярослав Юрьевич**

**Выпускная квалификационная работа**

# Алгебраические и полуалгебраические системы доказательств, использующие алгебраические схемы

Образовательная программа бакалавриат «Математика»
Направление и код: 01.03.01 «Математика»
Шифр ОП: СВ.5000.2016

Научный руководитель:
Профессор
Факультет математики
и компьютерных наук СПбГУ
доктор ф.-м. наук
Гирш Эдуард Алексеевич

Рецензент:
Assistant Professor
University of California at San Diego
кандидат ф.-м. наук
Кноп Александр Анатольевич

Санкт-Петербург
2020 год

**Аннотация**

Мы рассмотрим несколько обобщений системы доказательств Polynomial Calculus, а именно систему Ideal Proof System [4], в которой полиномы записываются в виде алгебраической схемы, систему Ext-PCR, в которой мы разрешаем вводить дополнительные переменные, обозначающие полиномы от изначальных переменных, систему Depth-inf-PC [23] , в которой мы разрешаем вводить дополнительные переменные, обозначающие произвольные полиномы.

В предположении гипотезы Шуба-Смейла [11] о том, что не существует арифметической схемы размера $(\log(n)+b)^c$ для вычисления $c_n n!$, мы докажем условную экспоненциальную нижнюю оценку на размер опровержений системы полиномиальных равенств $\mathsf{BVP}_n$ [18] в системе $\mathsf{IPS}_{\mathbb{Q}}$. $\mathsf{BVP}_n$ включает в себя равенство вида $\sum x_i 2^{i-1}+1=0$ и булевы аксиомы вида $x_i^2 - x_i = 0$.

Кроме того, мы докажем нижнюю оценку на размер доказательства $\mathsf{BVP}_n$ в системе Ext-PCR. После этого мы докажем, что система Ext-PCR полиномиально моделирует систему Res(Lin) [12] в случае, когда коэффициенты не превосходят полинома от размера доказательства. Из этого моделирования мы получим верхние оценки в системе Ext-PCR, тем самым окажется, что система Ext-PCR строго сильнее Polynomial Calculus. Наконец, мы покажем, что система Depth-inf-PC полиномиально моделирует систему Res(Lin).

# Содержание



# 1 Введение

Изучение сложности пропозициональных доказательств началось по существу со статьи С. А. Кука и Р. Рекхоу [1]. Поскольку общий вопрос о существовании системы доказательств, в которой у каждой формулы есть доказательство полиномиальной длины, эквивалентен NP = coNP, исследования ведутся для определенных систем. Программой Кука в теории сложности вычислений называется изучение сложности вывода во всё более сильных системах доказательств.

Алгебраические системы доказательств (основанные на выводе элемента идеала, порождённого исходными полиномами, то есть на теореме Гильберта о нулях) были впервые подробно рассмотрены в статье П.Бима, Р. Импальяццо и др. [2], в которой были доказаны нижние оценки для системы Nullstellensatz.

**Определение.** (Nullstellensatz) Пусть $\mathbb{F}$ — алгебраически замкнутое поле. Доказательством неразрешимости системы полиномиальных равенств $F_1(\vec{x}) = F_2(\vec{x}) = \cdots = F_m(\vec{x}) = 0$ над $\mathbb{F}$ в системе доказательств Nullstellensatz является последовательность полиномов $G_1, \ldots, G_m$, что

$$F_1G_1 + F_2G_2 + \ldots + F_nG_n = 1$$

В докладе на ICM-1998 Т. Питасси предложила исследовать алгебраические системы, в которых полиномы записываются алгебраическими формулами или схемами, в дальнейшем эта тема получила развитие в работе Э. А. Гирша и Д. Ю. Григорьева [3]. Д. Грошов и Т. Питасси [4] предложили общее определение системы, основанной на выводе в идеале, Ideal Proof System.

**Определение.** (Ideal Proof System). Пусть $\mathbb{F}$ — алгебраически замкнутое поле. $\mathsf{IPS}_{\mathbb{F}}$-сертификатом того факта, что система полиномиальных равенств $F_1(\vec{x}) = F_2(\vec{x}) = \cdots = F_n(\vec{x}) = 0$ неразрешима над $\mathbb{F}$, мы будем называть полином $C(\vec{x}, \vec{y}) \in \mathbb{F}[\vec{x}, \vec{y}]$ от переменных $x_1, \ldots, x_n$ и $y_1, \ldots, y_m$ такой, что:

1. $C(x_1, \ldots, x_n, \vec{0}) = 0$
2. $C(x_1, \ldots, x_n, F_1(\vec{x}), \ldots, F_m(\vec{x})) = 1$

Стоит заметить, что при записи доказательств в виде алгебраических схем получаются системы, не являющиеся системами доказательств в строгом смысле Кука–Рекхоу, так как неизвестно, как записанное в таком виде тождество проверить за полиномиальное время. Однако это можно сделать вероятностно, и такого рода системы рассматриваются со времен работы Т. Питасси [5].

Полуалгебраическими системами называются системы доказательств, основанные на полиномиальных неравенствах. П. Пудлак [20] сформулировал первые из этих систем, взяв за основу конструкции Ловаса и Схрайвера [19] для решения задач комбинаторной оптимизации. Первые нижние оценки были доказаны в работах Д. Григорьева, Э. А. Гирша, Д. В. Пасечника [6, 7, 8]. Э.А.Гирш на семинаре в Обервольфахе [9] поставил вопрос, эквивалентны ли эти системы алгебраическим в случае, когда полиномы записываются алгебраическими схемами. Э.А.Гирш и И.Цамерет [10] показали, что этот вопрос тесно связан с возможностью построения короткого вывода в IPS для системы, выражающей неотрицательность значения битовой записи (в дальнейшем, данную систему полиномиальных равенств мы будем называть *Binary Value Principle*, сокращенно $\mathsf{BVP}_n$):

$$\sum_{i=1}^{n} x_i 2^{i-1} + 1 = 0,\ x_1^2 - x_1 = 0,\ \ldots,\ x_n^2 - x_n = 0 \qquad (*)$$

Д.Ю.Григорьев выдвинул гипотезу [25], что нижнюю оценку возможно доказать в предположении тау-гипотезы Блюм–Шуба–Смейла [11] (отрицательная сверхзадача), и показал это для доказательств системы, отличающейся заменой первого полинома на $\sum_{i=1}^{n} x_i 2^{i-1} + y$, над рациональными функциями от $y$.

В первой главе мы расширим определение IPS для колец $\mathbb{Z}$ и $\mathbb{Q}$ и докажем, что если система полиномов $(*)$ имеет короткое доказательство в системе IPS над $\mathbb{Z}$ или над $\mathbb{Q}$, записанное в виде алгебраической схемы, то не выполняется другая гипотеза Шуба–Смейла, а именно, что для любой последовательности вида $\{c_n n!\}, c_n \in \mathbb{Z}, c_n \neq 0$ не существует арифметической схемы размера $poly(n)$, которая ее вычисляет. Следовательно, в этом предположении система IPS не моделирует полиномиально полуалгебраические доказательства, так как в любой полуалгебраической системе доказательств есть опровержение полиномиального размера для системы $(*)$. Эта оценка, вместе с упомянутыми выше результатами Э. Гирша, Д. Григорьева и И. Цамерета, опубликована в статье [18].

Помимо статических систем доказательств вроде Nullstellensatz, часто рассматривают динамические версии алгебраических систем доказательств. Динамические системы отличаются от статических тем, что в них вывод представляет собой последовательность вычислений которые производятся согласно с заранее заданными правилами вывода. Наиболее известной из таких систем является система Polynomial Calculus.

**Определение.** Пусть $\{P_1, \ldots, P_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$ — набор полиномов такой, что система полиномиальных равенств $P_1 = 0, \ldots, P_m = 0$ не имеет решения. Тогда опровержением для $\{P_1, \ldots, P_m\}$ в системе доказательств Polynomial Calculus называется последовательность полиномов $R_1, \ldots, R_s \in \mathbb{F}[x_1, \ldots, x_n]$, где $R_s = 1$ и любой полином $R_l$ удовлетворяет одному из следующих соотношений:

- $R_l = P_i$ для некоторого $i \in \{1, \ldots, m\}$
- $R_l = \alpha R_j + \beta R_i$ где $\alpha, \beta \in \mathbb{F}$, $i, j < l$
- $R_l = x_i R_j$ где $j < l$

Размером доказательства мы будем называть $\sum_{l=1}^{s} size(R_l)$, где $size(R_l)$ — это количество битов, необходимых для записи полинома $R_l$ (то есть суммарное количество битов, необходимое для записи всех коэффициентов входящих в него мономов).

В статьях [15], [16] были доказаны различные экспоненциальные нижние оценки для данной системы доказательств. В статье Р. Импальяццо, С. Мули, Т. Питасси [23] была рассмотрена система ΣΠΣ-PC, которая являются обобщением системы Polynomial Calculus.

**Определение.** Пусть $\{P_1, \ldots, P_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$ — набор полиномов такой, что система полиномиальных равенств $P_1 = 0, \ldots, P_m = 0$ не имеет решения. Пусть $Q_1, \ldots, Q_k \in \mathbb{F}[x_1, \ldots, x_n]$ — некоторые полиномы, которые имеют вид $Q_j = a_{0j} + \sum_i a_{ij} x_i$, где $a_{ij} \in \mathbb{F}$. Тогда опровержением в системе ΣΠΣ-PC мы будем называть PC-опровержение системы $\{P_1, \ldots, P_m, y_1 - Q_1, \ldots, y_k - Q_k\}$, где $y_i$ — новые переменные.

Для системы ΣΠΣ-PC было доказано, что она полиномиально моделирует систему CP*. Также легко заметить, что система IPS полиномиально моделирует систему ΣΠΣ-PC в случае, когда полиномы записываются в виде алгебраической схемы. Во второй главе мы рассмотрим систему менее общую, чем IPS, но являющуюся обобщением системы ΣΠΣ-PC, а именно Ext-PCR. Данная система отличается от ΣΠΣ-PC тем, что мы не накладываем ограничений на полиномы $Q_i$.

**Определение.** Пусть $\Gamma = \{P_1, \ldots, P_m\}$ — набор полиномов над переменными $x_1, \ldots, x_n$ в поле $\mathbb{F}$ такой, что система полиномиальных равенств $P_1 = 0, \ldots, P_m = 0$ не имеет решения. Пусть $Q_1, \ldots, Q_k \in \mathbb{F}[x_1, \ldots, x_n]$ — произвольные полиномы. Тогда опровержением в системе Ext-PCR мы будем называть PC-опровержение системы $\{P_1, \ldots, P_m, y_1 - Q_1, \ldots, y_k - Q_k\}$, где $y_i$ — новые переменные.

В статье Р. Импальяццо, С. Мули, Т. Питасси [23] было сформулировано два открытых вопроса:

- Существуют ли нижние оценки на размер доказательства в системе Polynomial Calculus, не использующие нижнюю оценку на степень доказательства в этой системе.
- Существуют ли нижние оценки на размер доказательства в системе ΣΠΣ-PC.

Во второй главе мы дадим ответ на оба эти вопроса. Мы докажем безусловную экспоненциальную нижнюю оценку на размер опровержения BVP (система полиномиальных равенств $(*)$) в системе Ext-PCR. При этом для доказательство не использует нижние оценки на степень доказательства. Кроме того, мы докажем, что система $\text{Ext-PCR}_{\mathbb{Q}}$ полиномиально моделирует систему доказательств $\text{Res}(\text{Lin}_{\mathbb{Q}})$ (впервые представлена в статье Р. Раза, И. Цамерета [12]) при условии, что все коэффициенты, появляющиеся в ходе доказательства, целые и не превосходят полинома от размера доказательства. Из этого факта мы получим в качестве следствия полиномиальную верхнюю оценку на размер опровержения формул Pigeon Hole Princliple ($\text{PHP}_n^m$), которые впервые были предложены в статье А. Хакена [22], и цейтинских формул ($\text{TS}_{G,f}$), которые впервые были предложены в статье Г. С. Цейтина [21]. Из полученных верхних оценок будет следовать, что система Ext-PCR строго сильнее, чем система PCR.

Также в статье Р. Импальяццо, С. Мули, Т. Питасси [23] рассматривалась система доказательств Depth-d-PC.

**Определение.** SLP S над переменными $x_1, \ldots, x_n$ в поле $\mathbb{F}$ мы будем называть последовательность вычислений $y_1, \ldots, y_k$ где каждая $y_j$ вычисляется по одному из следующих правил:

- $y_j = x_i$ для некоторого $i \in \{1, \ldots, n\}$
- $y_j = \sum_{l \in \{1,\ldots,j-1\}} \alpha_l y_l$, где $\alpha_l \in \mathbb{F}$
- $y_j = \prod_{l \in C_j} y_l$, где $C_j \subseteq \{1, \ldots, j-1\}$

Рассмотрим SLP S как ориентированный ациклический граф с гейтами помеченными как сумма или произведение и листьями помеченными как переменные $x_i$. Тогда глубина $S$ — это длина наибольшего ориентированного пути в этом графе от корня до листа.

**Определение.** Пусть $\{P_1, \ldots, P_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$ — набор полиномов такой, что система полиномиальных равенств $P_1 = 0, \ldots, P_m = 0$ не имеет решения. Пусть $S = (y_1, \ldots, y_k)$ - SLP над переменными $x_1, \ldots, x_n$ глубины $d-2$, определенная при помощи равенств

$$y_j = Q_j(x_1, \ldots, x_n, y_1, \ldots, y_{j-1}).$$

Тогда опровержением в системе Depth-d-PC мы будем называть PC-опровержение системы

$$\{P_1, \ldots, P_m, y_1 - Q_1, \ldots, y_k - Q_k\},$$

где $y_i$ — новые переменные.

Легко заметить, что система Ext-PCR занимает промежуточное положение между Depth-4-PC и Depth-5-PC. При этом в статье [23] было доказано, что Depth-43-PC полиномиально моделирует системы Cutting Planes и Positivestellensatz Calculus над полем $\mathbb{F}_{p^m}$ для любого простого $p$ и степени $m$, логарифмически зависящей от числа мономов в каждой строчке доказательства.

В третьей главе мы рассмотрим систему доказательств Depth-inf-PC. Данная система является обобщением Depth-$d$-PC для случая, когда глубина SLP не ограничена.

**Определение.** Пусть $\{P_1, \ldots, P_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$ — набор полиномов такой, что система полиномиальных равенств $P_1 = 0, \ldots, P_m = 0$ не имеет решения. Пусть $Q_1, \ldots, Q_k$ — полиномы, такие что $Q_i \in \mathbb{F}[x_1, \ldots, x_n, y_1, \ldots, y_{i-1}]$ для любого $i \geq 1$ (при $i = 1$ полином $Q_1 \in \mathbb{F}[x_1, \ldots, x_n]$). Тогда опровержением в системе $\text{Depth-inf-PC}_{\mathbb{F}}$ мы будем называть $\text{PC}_{\mathbb{F}}$-опровержение системы $\{P_1, \ldots, P_m, y_1 - Q_1, \ldots, y_k - Q_k\}$, где $y_i$ — новые переменные.

Для этой системы мы докажем, что она полиномиально моделирует систему доказательств $\text{Res}(\text{Lin}_{\mathbb{Q}})$ в случае, когда система полиномиальных равенств порождена булевой формулой.

# 2 Нижняя оценка в Ideal Proof System

## 2.1 Основные определения

Для того, чтобы перевести формулу $F$ в $k$-КНФ, мы переведем каждый дизъюнкт $F$ в полиномиальное равенство. А именно, любой дизъюнкт, состоящий из переменных $v_1, \ldots, v_t (t \leq k)$, будет переведен в следующее полиномиальное равенство:

$$l_1 \ldots l_t = 0,$$

где $l_i = 1 - v_i$, если переменная входит в наш дизъюнкт без отрицания, и $l_i = v_i$, если переменная входит в дизъюнкт с отрицанием. Также для каждой переменной $v_i$ мы добавим в нашу систему равенство вида $v_i^2 - v_i = 0$. Согласно определению IPS, данному во введении:

**Определение.** (Ideal Proof System). Пусть $\mathbb{F}$ — алгебраически замкнутое поле. $\mathsf{IPS}_{\mathbb{F}}$-сертификатом того факта, что система полиномиальных равенств $F_1(\vec{x}) = F_2(\vec{x}) = \cdots = F_n(\vec{x}) = 0$ неразрешима над $\mathbb{F}$, мы будем называть полином $C(\vec{x}, \vec{y}) \in \mathbb{F}[\vec{x}, \vec{y}]$ от переменных $x_1, \ldots, x_n$ и $y_1, \ldots, y_m$ такой, что:

1. $C(x_1, \ldots, x_n, \vec{0}) = 0$
2. $C(x_1, \ldots, x_n, F_1(\vec{x}), \ldots, F_m(\vec{x})) = 1$

В данной работе мы рассмотрим вариант IPS в том случае, когда $\mathbb{F} = \mathbb{Z}$ или $\mathbb{F} = \mathbb{Q}$. В случае $\mathbb{F} = \mathbb{Q}$ определение IPS не меняется за исключением того факта, что $\mathbb{Q}$ не является алгебраически замкнутым полем. В случае же $\mathbb{F} = \mathbb{Z}$ определение немного изменится.

**Определение.** (Ideal Proof System над $\mathbb{Z}$). $\mathsf{IPS}_{\mathbb{Z}}$-сертификатом того факта, что система полиномиальных равенств $F_1(\vec{x}) = F_2(\vec{x}) = \cdots = F_n(\vec{x}) = 0$ неразрешима над $\mathbb{Z}$, мы будем называть полином $C(\vec{x}, \vec{y}) \in \mathbb{Z}[\vec{x}, \vec{y}]$ над переменными $x_1, \ldots, x_n$ и $y_1, \ldots, y_m$ такой, что:

1. $C(x_1, \ldots, x_n, \vec{0}) = 0$
2. $C(x_1, \ldots, x_n, F_1(\vec{x}), \ldots, F_m(\vec{x})) = M$, где $M \in \mathbb{Z}, M \neq 0$

**Замечание.** Обычно, когда речь идет об Ideal Proof System, полнота системы доказывается при помощи Nullstellensatz theorem(теорема Гильберта о нулях). Но в случае, когда мы работаем над $\mathbb{Z}$ или над $\mathbb{Q}$ мы не можем использовать эту теорему, так как $\mathbb{Z}$ и $\mathbb{Q}$ не являются алгебраически замкнутыми полями. Докажем полноту $\mathsf{IPS}_{\mathbb{Z}}$ в случае, когда переменные булевы. Пусть система полиномиальных равенств

$$F_1(\overline{x}) = F_2(\overline{x}) = \ldots = F_m(\overline{x}) = x_1^2 - x_1 = x_2^2 - x_2 = \ldots = x_n^2 - x_n,$$

где $F_j \in \mathbb{Z}[x_1, \ldots, x_n]$, не имеет решений для $x_i \in \mathbb{Z}$. Тогда докажем, что существует $\mathsf{IPS}_{\mathbb{Z}}$-сертификат $C(\overline{x}, \overline{y})$ для данной системы полиномиальных равенств. Если мы докажем, что существуют такие полиномы $P_1, P_2, \ldots, P_m, Q_1, \ldots, Q_n \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, что

$$F_1 \cdot P_1 + F_2 \cdot P_2 + \ldots + F_m \cdot P_m + (x_1^2 - x_1) \cdot Q_1 + \ldots (x_n^2 - x_n) \cdot Q_n = M \tag{1}$$

для некоторой целой константы $M \neq 0$, то из этого будет очевидно следовать существование $\mathsf{IPS}_{\mathbb{Z}}$-сертификата для нашей системы полиномиальных равенств.

Легко заметить, что

$$1 = (x_1 + (1 - x_1)) \cdot (x_2 + (1 - x_2)) \cdots (x_n + (1 - x_n)) \tag{2}$$

Тогда, если мы докажем, что для любого полинома вида $l_1 \cdot l_2 \cdots l_n$, где $l_i = x_i$ или $l_i = 1 - x_i$, существуют полиномы $P'_1, P'_2, \ldots, P'_m, Q'_1, \ldots, Q'_n \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, такие что

$$F_1 \cdot P'_1 + F_2 \cdot P'_2 + \ldots + F_m \cdot P'_m + (x_1^2 - x_1) \cdot Q'_1 + \ldots (x_n^2 - x_n) \cdot Q'_n = M' \cdot l_1 \cdot l_2 \cdots l_n,$$

то из равенства (2) будет очевидно следовать существование полиномов $P_1, P_2, \ldots, P_m, Q_1, \ldots, Q_n \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, для которых равенство (1) выполнено.

Рассмотрим любой полином вида $l_1 \cdot l_2 \cdots l_n$, где $l_i = x_i$ или $l_i = 1 - x_i$. Рассмотрим вектор $t_1, t_2 \ldots t_n$ такой, что $t_i \in \{0, 1\}$ и $l_i(t_i) = 0$ (то есть $t_i$ это те значения $x_i$, при которых $l_i$ обнуляется). Тогда, так как наша система $\{F_1, \ldots, F_m\}$ не имеет решения для всех булевых значений $x_1, \ldots, x_n$, для некоторого $j \in [m]$ верно, что $F_j(t_1, \ldots, t_m) \neq 0$. Тогда, если мы рассмотрим полином $F_j \cdot l_1 \cdot l_2 \cdots l_n$ и сократим все переменные $x_i^2$ в каждом из мономов, используя равенства $x_i^2 - x_i = 0$, мы получим полином $F_j(t_1, \ldots, t_n) \cdot l_1 \cdot l_2 \cdots l_n$, где $F_j(t_1, \ldots, t_n) \in \mathbb{Z}$, $F_j(t_1, \ldots, t_n) \neq 0$, чего мы и добивались.

Аналогичный подход может быть использован для доказательства полноты системы $\mathsf{IPS}_{\mathbb{Q}}$.

**Определение.** Вычислением длины $l$ данного целого числа $m$ называется последовательность целых чисел $x_0, \ldots, x_l$, где $x_0 = 1, x_l = m$, и для любого $1 \leq k \leq m$ существуют такие индексы $0 \leq i, j < k$ такие, что $x_k = x_i \circ x_j$, где $\circ$ это сложение, вычитание или умножение. Такую последовательность также называют арифметической схемой, вычисляющей $m$. Мы также определим функцию $\tau : \mathbb{Z} \longrightarrow \mathbb{N}$ такую, что $\tau(m)$ — это минимальная длина вычисления $m$.

**Определение.** Бесконстантной $\mathbb{Z}$-алгебраической схемой, вычисляющей полином $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$, называется последовательность полиномов $g_1, \ldots, g_m = f$, где каждый полином $g_i$ (их также называют гейтами) либо равен некоторой переменной $x_i$, либо равен одной из констант $\{0, 1, -1\}$, либо имеет вид $g_i \circ g_k$ для некоторых $j, k < i$, где $\circ$ обозначает сумму или умножение. Мы определим размер алгебраической схемы как количество гейтов в схеме.

В дальнейшем, нам понадобится определение алгебраической схемы над $\mathbb{Q}$.

**Определение.** Бесконстантной $\mathbb{Q}$-алгебраической схемой, вычисляющей полином $f(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ мы будем называть обычную бесконстантную $\mathbb{Q}$-алгебраическую схему, в которую также добавлены гейты деления $\div$, где $u \div v$ обозначает, что полином $u$ делится на полином $v$. При этом для каждого гейта $u \div v$ мы потребуем, что схема, считающая $v$, не содержит переменных $x_1, \ldots x_n$. Тогда размером схемы мы будем считать количество гейтов схемы.

**Замечание.** Заметим, что для любого целого числа $m$ существует арифметическая схема размера $\log m$, вычисляющая его. Поэтому, если нам дана бесконстантная $\mathbb{Z}$-алгебраическая схема размера $M$, считающая полином $F(x_1, \ldots, x_n)$, то для любого целого вектора $(y_1, \ldots, y_n)$ существует арифметическая схема размера $(M + \sum \log y_i)$, считающая $F(y_1, \ldots, y_n)$.

## 2.2 Нижняя оценка

Сначала сформулируем гипотезу Шуба–Смейла:

**Гипотеза.** Не существует констант $a, b > 0$ таких, что для некоторой последовательности $\{c_n\}$, где $c_n \in \mathbb{Z}, c_n \neq 0$ выполнено неравенство

$$\tau(c_n n!) \leq (\log n + a)^b$$

**Теорема 1.** Предположим, что система полиномиальных равенств $G(\vec{x}) = F_1(\vec{x}) = F_2(\vec{x}) = \cdots = F_n(\vec{x}) = 0$, где $G(\vec{x}) = 1 + \sum_{i=1}^{i=n} 2^{(i-1)} x_i$ и $F_i(\vec{x}) = x_i^2 - x_i$, имеет $\mathsf{IPS}_{\mathbb{Z}}$-сертификат $C(\vec{x}, \vec{y})$, который может быть вычислен с помощью бесконстантной $\mathbb{Z}$-алгебраической схемы размера $poly(n)$. Тогда гипотеза Шуба–Смейла не выполняется, а именно, существует последовательность $\{c_n n!\}$, где $c_n \in \mathbb{Z}, c_n \neq 0$ и $\tau(c_n n!) \leq (\log n + a)^b$, где $a$ и $b$ — константы.

**Доказательство.** По определению $\mathsf{IPS}_{\mathbb{Z}}$-сертификата существует константа $M \in \mathbb{Z}, M \neq 0$ такая, что

$$C(x_1, \ldots, x_n, G(\vec{x}), F_1(\vec{x}), \ldots, F_n(\vec{x})) = M$$

Тогда для любого целого числа $0 \leq k < 2^n$ существует битовый вектор $(x_{k1}, \ldots, x_{kn})$ такой, что $k = \sum_{i=1}^{i=n} x_{ki} 2^{i-1}$. Тогда $F_i(\vec{x}_k) = 0, G(\vec{x}_k) = 1 + k$ для каждого $1 \leq i \leq n$, $0 \leq k < 2^n$. Значит $C(x_{k1}, \ldots, x_{kn}, k, \vec{0}) = M$ для любого целого $1 \leq k \leq 2^n$. При этом $C(x_{k1}, \ldots, x_{kn}, 0, \vec{0}) = 0$ по определению $\mathsf{IPS}_{\mathbb{Z}}$-сертификата. Значит если зафиксировать $x_{k1}, \ldots, x_{kn}$ и последние $n$ координат, то получится $\mathbb{Z}$-полином по оставшейся координате, который в точке 0 равен 0, а в точке $k$ равен $M$. Таким образом $M$ делится на $k$ для любого целого $1 \leq k \leq 2^n$. Тогда $M$ делится на любое простое число $p < 2^n$.

Теперь покажем, что существует арифметическая схема размера $poly(n)$, считающая $M$. Действительно, заметим что для этого достаточно просто подставить $x_0 = \vec{0}$ в алгебраическую схему для $C(\vec{x}_0, G(\vec{x}_0), F(\vec{x}_0))$ и получить арифметическую схему, считающую константу $M$. Поэтому мы знаем, что для $M$ существует схема размера $poly(n)$.

Если же существует арифметическая схема размера $poly(n)$, считающая $M$, то существует схема размера $poly(n)$, считающая $M^{2^n}$, так как мы можем возвести $M$ в степень $2^n$ просто возведя $M$ в квадрат $n$ раз.

Для любого простого числа $p$, его степень вхождения в разложение числа $(2^n)!$ считается как $\lfloor \frac{2^n}{p} \rfloor + \lfloor \frac{2^n}{p^2} \rfloor + \lfloor \frac{2^n}{p^3} \rfloor + \ldots$, что очевидно не больше чем $\frac{2^n}{p-1} \leq 2^n$. Тогда используя тот факт, что $M^{2^n}$ делится на $p^{2^n}$ для любого простого числа $p < 2^n$, получаем, что существует арифметическая схема размера $poly(n)$, считающая некоторое число, кратное $(2^n)!$. То есть существует последовательность $\{c_{2^n}(2^n)!\}$ такая, что $\tau(c_{2^n}(2^n)!) \leq (n + a)^b$ для некоторых констант $a$ и $b$.

Для каждого $m \in \mathbb{N}$ существует целое $n$ такое, что $2^{n-1} \leq m < 2^n$. Тогда в качестве $c_m m!$ можно взять просто $c_{2^n}(2^n)!$. Тогда $\tau(c_m m!) \leq (n + a)^b \leq (\log(2m + a)^b \leq (\log m + a)^c$ для некоторых констант $a, b$ и $c$. □

**Теорема 2.** Предположим, что система полиномиальных равенств $G(\vec{x}) = F_1(\vec{x}) = F_2(\vec{x}) = \cdots = F_n(\vec{x}) = 0$, где $G(\vec{x}) = 1 + \sum_{i=1}^{i=n} 2^{(i-1)} x_i$ и $F_i(\vec{x}) = x_i^2 - x_i$, имеет $\mathsf{IPS}_{\mathbb{Q}}$-сертификат $C(\vec{x}, \vec{y})$, который может быть посчитан с помощью бесконстантной $\mathbb{Q}$-алгебраической схемы размера $poly(n)$. Тогда гипотеза Шуба–Смейла не выполняется, а именно, существует последовательность $\{c_n n!\}$, где $c_n \in \mathbb{Z}, c_n \neq 0$ и $\tau(c_n n!) \leq (\log n + a)^b$, где $a$ и $b$ — константы.

*Доказательство.* Пусть $g_1, \ldots, g_t = C$ — это бесконстантная $\mathbb{Q}$-алгебраическая схема, вычисляющая $C$.

Мы покажем по индукции, что для данной $\mathbb{Q}$-алгебраической схемы размера $poly(n)$, вычисляющей $C$, существует арифметическая схема размера $poly(n)$, вычисляющая некоторую целую константу $M \neq 0$ такую, что существует $\mathbb{Z}$-алгебраическая схема размера $poly(n)$, считающая $M \cdot C$.

**Индукционное предположение:** Пусть последовательность полиномов $g_1, \ldots, g_s \in \mathbb{Q}[\vec{x}, \vec{y}]$ образует бесконстантную $\mathbb{Q}$-алгебраическую схему. Тогда существует последовательность полиномов

$$g_{11}, \ldots, g_{1a_1}, g_{21}, \ldots, g_{2a_2}, \ldots, g_{s1}, \ldots, g_{sa_s} \in \mathbb{Z}[\vec{x}, \vec{y}],$$

образующая бесконстантную $\mathbb{Z}$-алгебраическую схему, такую что для любого $i \leq s$:

1. $a_i \leq 4$ и $g_{ia_i} = M_i \cdot g_i$ для некоторой целой константы $M_i$.

2. У нашей последовательности полиномов $g_{11}, \ldots, g_{1a_1}, g_{21}, \ldots, g_{2a_2}, \ldots, g_{s1}, \ldots, g_{sa_s}$ есть некоторая подпоследовательность, в которой встречаются все константы $M_i$, и эта подпоследовательность образует корректную бесконстантную $\mathbb{Z}$-алгебраическую схему, не содержащую переменных (то есть внутри нашей схемы есть арифметическая схема, вычисляющая все константы $M_i$)

**База:** Если $t = 1$, то $g_1 \in \{0, 1, -1\}$ или $g_1$ - это переменная. Тогда $a_1 = 2$, $g_{11} = 1$, $g_{12} = g_1$ и $M_1 = 1$.

**Переход:** Пусть мы уже построили для всех $i < k$ арифметическую схему, считающую $M_i$, и $\mathbb{Z}$-алгебраическую схему, считающую $M_i \cdot g_i$. Теперь построим схемы для $k$. Возможны 2 случая:

1. если $g_k = x_i$ для некоторого $i$, то $a_k = 2$, $g_{k1} = 1$, $g_{k2} = x_i$, то есть $M_i = 1$.

2. Пусть $g_k = g_i \circ g_j$, где $i, j < k$. Тогда в этом случае есть еще 3 подслучая:

   (a) Пусть $g_k = g_i \cdot g_j$. Тогда в качестве $M_k$ можно взять $M_i \cdot M_j$. Тогда $M_k \cdot g_k = (M_i \cdot g_i) \cdot (M_j \cdot g_j)$. Значит, мы можем взять $a_k = 2$, $g_{k1} = M_i \cdot m_j$, $g_{k2} = g_{ja_j} \cdot g_{la_l}$.

   (b) Пусть $g_k = g_i + g_j$. Тогда $a_k = 4$,

   $$g_{k1} = M_k = M_i M_j,\ g_{k4} = M_l \cdot g_{ja_j} + M_j \cdot g_{la_l},\ g_{k1} = M_i \cdot M_j,$$

   а гейты $g_{k2}$ и $g_{k3}$ нам нужны для реализации промежуточных вычислений.

   (c) Пусть $g_k = g_i \div g_j$. Тогда $a_k = 2$,

   $$g_{k2} = M_j g_{ia_i},\ g_{k1} = M_k = M_i \cdot g_{ja_j}.$$

   Очевидно, индукционное предположение останется верным, так как $g_{ja_j}$ — некоторая целая константа.

Таким образом в качестве $M$ можно взять $M_t$, а в качестве $M \cdot C$ можно взять $g_{ta_t}$ соответственно. Тогда размер соответствующих им схем $poly(n)$, так как в получившейся схеме не более $4t$ гейтов. Тогда, используя тот факт, что $M \cdot C$ — это $\mathsf{IPS}_{\mathbb{Z}}$-сертификат для системы $\mathbb{Z}$-полиномиальных равенств $G(\vec{x}) = F_1(\vec{x}) = F_1(\vec{x}) = \ldots = F_n(\vec{x}) = 0$, мы можем закончить доказательство, используя теорему 1.

□

# 3 Система доказательств Ext-PCR, нижние и верхние оценки

## 3.1 Определения

Для начала определим систему $\mathsf{Res}(\mathsf{lin}_{\mathsf{R}})$, она нам понадобится для получения верхней оценки в секции 3.4.

**Определение.** Для кольца $R$ система $\mathsf{Res}(\mathsf{lin}_{\mathsf{R}})$ является обобщением резолюционной системы доказательств. Пусть нам дана формула $F$ в $k$-КНФ. Тогда каждый дизъюнкт, состоящий из переменных $v_1, \ldots, v_t$ $(t \leq k)$, будет записан в следующей форме:

$$(l_1 = 0) \vee \ldots \vee (l_t = 0),$$

где $l_i = 1 - v_i$, если переменная входит в наш дизъюнкт без отрицания, и $l_i = v_i$, если переменная входит в дизъюнкт с отрицанием. Также мы добавим в список аксиом все дизъюнкции вида

$(x = 0) \vee (x = 1)$. Строчками в нашем выводе будут дизъюнкции линейных равенств, при этом одно и то же равенство может возникать в строчке несколько раз. При этом мы считаем, что линейные равенства в сточке не упорядочены.

Теперь определим правила вывода в системе $\mathsf{Res}(\mathsf{lin}_\mathsf{R})$:

1. Основное правило вывода в системе $\mathsf{Res}(\mathsf{lin}_\mathsf{R})$ будет выглядеть так: из $C \vee (f = 0)$ и $D \vee (g = 0)$ мы можем вывести $C \vee D \vee (\alpha f + \beta g = 0)$.
2. Из $C \vee (k = 0)$ мы можем вывести $C$, если $k \in R, k \neq 0$.
3. Из формул вида $C \vee (f = 0) \vee (f = 0)$ можем вывести $C \vee (f = 0)$.

Доказательством в системе $\mathsf{Res}(\mathsf{lin}_\mathsf{R})$ является вывод $k = 0$ из аксиом, где $k \in R, k \neq 0$. Размером доказательства $\mathsf{Res}(\mathsf{lin}_\mathsf{R})$ будем называть суммарный размер всех дизъюнктов, участвующих в доказательстве. Размером же каждого дизъюнкта мы будем считать суммарное число битов, необходимых для его записи.

Теперь вернемся к системам доказательств, основанным на полиномиальных равенствах. Для этого нам нужно определить, как именно мы будем записывать формулы в виде полиномов.

Как и в случае с IPS, чтобы перевести формулу $F$ в форме $k$-КНФ, мы переведем каждый дизъюнкт $F$ в полиномиальное равенство. А именно, любой дизъюнкт, состоящий из переменных $v_1, \ldots, v_t (t \leq k)$, будет переведен в следующее полиномиальное равенство:

$$l_1 \ldots l_t = 0,$$

где $l_i = \overline{v_i}$, если переменная входит в наш дизъюнкт без отрицания, и $l_i = v_i$, если переменная входит в дизъюнкт с отрицанием. Также, для каждой переменной мы добавим в нашу систему равенства вида $v_i^2 - v_i = 0$ и $v_i = 1 - \overline{v_i}$. Согласно определению PC, данному во введении:

**Определение.** Пусть $\{P_1, \ldots, P_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$ — набор полиномов такой, что система полиномиальных равенств $P_1 = 0, \ldots, P_m = 0$ не имеет решения. Тогда опровержением для $\Gamma$ в системе доказательств Polynomial Calculus называется последовательность полиномов $R_1, \ldots, R_s \in \mathbb{F}[x_1, \ldots, x_n]$, где $R_s = 1$ и любой полином $R_l$ удовлетворяет одному из следующих соотношений:

- $R_l = P_i$ для некоторого $i \in \{1, \ldots, m\}$
- $R_l = \alpha R_j + \beta R_i$ где $\alpha, \beta \in \mathbb{F}$, $i, j < l$
- $R_l = x_i R_j$ где $j < l$

Размером доказательства мы будем называть $\sum_{l=1}^{s} size(R_l)$, где $size(R_l)$ — это количество битов, необходимых для записи полинома $R_l$ (то есть суммарное количество битов, необходимое для записи всех коэффициентов входящих в него мономов).

**Замечание.** В случае, когда $\mathbb{F} = \mathbb{Q}$, размер любого коэффициента $\alpha = \frac{a}{b} \in \mathbb{Q}$ мы будем считать равным $\lceil \log(|a|) \rceil + \lceil \log(|b|) \rceil + 1$, то есть суммарное число битов, необходимых для записи числителя и знаменателя.

**Определение.** Пусть $\{P_1, \ldots, P_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$ — набор полиномов такой, что система полиномиальных равенств $P_1 = 0, \ldots, P_m = 0$ не имеет решения. Пусть $Q_1, \ldots, Q_k \in \mathbb{F}[x_1, \ldots, x_n]$ — произвольные полиномы. Тогда опровержением в системе Ext-PCR мы будем называть PC-опровержение системы $\{P_1, \ldots, P_m, y_1 - Q_1, \ldots, y_k - Q_k\}$, где $y_i$ - новые переменные. Размером Ext-PCR-опровержения для набора $\Gamma = \{P_1, \ldots, P_m\}$ мы будем называть наименьший возможный размер PC-опровержения для $\{P_1, \ldots, P_m, y_1 - Q_1, \ldots, y_k - Q_k\}$ по всем наборам $Q_1, \ldots, Q_k$.

**Замечание.** Полнота для системы $\mathsf{Ext\text{-}PCR}_\mathbb{Q}$ доказывается аналогично полноте для системы $\mathsf{IPS}_\mathbb{Z}$.

### 3.2 Нижняя оценка на BVP

Для получения нижней оценки для BVP над полем $\mathbb{Q}$ мы сначала рассмотрим вариант системы доказательств Ext-PCR над кольцом $\mathbb{Z}$. Для этого определим систему доказательств PC над кольцом $\mathbb{Z}$.

**Определение.** Пусть $\{P_1, \ldots, P_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$ — набор полиномов такой, что система полиномиальных равенств $P_1 = 0, \ldots, P_m = 0$ не имеет решения. Тогда опровержением для $\Gamma$ в системе доказательств Polynomial Calculus называется последовательность полиномов $R_1, \ldots, R_s \in \mathbb{F}[x_1, \ldots, x_n]$, где $R_s = M$, **а** $M$ — **некоторая целая константа**, и любой полином $R_l$ удовлетворяет одному из следующих соотношений:

- $R_l = P_i$ для $i \in \{1, \ldots, m\}$
- $R_l = \alpha R_j + \beta R_i$ для $\alpha, \beta \in \mathbb{Z}$, $i, j < l$
- $R_l = x_i R_j$ где $j < l$

Размером доказательства мы будем называть $\sum_{l=1}^{s} size(R_l)$, где $size(R_l)$ — это количество битов, необходимых для записи полинома $R_l$ (то есть суммарное количество битов, необходимое для записи его коэффициентов).

Тогда система $\text{Ext-PCR}_{\mathbb{Z}}$ определяется как и в случае поля, но с использованием системы $\text{PC}_{\mathbb{Z}}$.

**Теорема 3.** Рассмотрим систему полиномиальных равенств $G(\vec{x}) = F_1(\vec{x}) = F_2(\vec{x}) = \cdots = F_n(\vec{x}) = 0$, где $G(\vec{x}) = 1 + \sum_{i=1}^{i=n} 2^{(i-1)} x_i$ и $F_i(\vec{x}) = x_i^2 - x_i$. Тогда размер любого опровержения для такой системы в $\text{Ext-PCR}_{\mathbb{Z}}$ не меньше чем $C \cdot 2^n$. Более того, константа $M$, получающаяся в конце такого доказательства, имеет хотя бы $C \cdot 2^n$ битов в своей записи для некоторой фиксированной константы $C$.

**Доказательство.** Легко заметить, что каждый полином, получающийся в ходе нашего доказательства, представляется в виде $P_0 G + P_1 F_1 + \ldots + P_n F_n + H_1(y_1 - Q_1) + H_2(y_2 - Q_2) + \ldots + H_k(y_k - Q_k)$. Тогда мы знаем, что целая константа $M$, получающаяся в конце доказательства, представляется в виде

$$P_0 G + P_1 F_1 + \ldots + P_n F_n + H_1(y_1 - Q_1) + H_2(y_2 - Q_2) + \ldots + H_k(y_k - Q_k) = M$$

Для любого целого числа $0 \leq t < 2^n$ существует битовый вектор $(x_{t1}, \ldots, x_{tn})$ такой, что $t = \sum_{i=1}^{i=n} x_{ti} 2^{i-1}$. Тогда $F_i(\vec{x}_t) = 0, G(\vec{x}_t) = 1 + t$ для каждого $1 \leq i \leq n$, $0 \leq t < 2^n$. Подставим такие значения $y_i$, что $y_i = Q_i(\vec{x}_t)$. Значит $P_0(x_{t1}, \ldots, x_{tn}, y_1, \ldots, y_k) \cdot t = M$ для любого целого $1 \leq t \leq 2^n$. Таким образом $M$ делится на $t$ для любого целого $1 \leq t \leq 2^n$. Тогда $M$ делится на любое простое число $t < 2^n$. Тогда $M$ делится на произведение всех простых чисел не превосходящих $2^n$. Тогда очевидно, что $|M| > (\pi(2^n))!$. По теореме о распределении простых чисел мы знаем, что при достаточно больших $n$ выполнено $\pi(2^n) > C\frac{2^n}{n}$. Значит $|M| > (C\frac{2^n}{n})!$ при больших $n$. Применим формулу Стирлинга:

$$|M| > \left(C\frac{2^n}{n}\right)! > C' \cdot \left(C\frac{2^n}{n}\right)^{C\frac{2^n}{n}} > C'' \left(2^{\frac{n}{2}}\right)^{C\frac{2^n}{n}} > C'' 2^{(2^n C_0)}$$

Значит для записи константы $M$ потребуется хотя бы $C_1 \cdot 2^n$ битов. Значит и размер доказательства был экспоненциальным, так как в запись доказательства должна быть включена запись константы $M$. $\square$

Теперь мы докажем нижнюю оценку для системы $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$.

**Теорема 4.** Рассмотрим систему полиномиальных равенств $G(\vec{x}) = F_1(\vec{x}) = F_2(\vec{x}) = \cdots = F_n(\vec{x}) = 0$, где $G(\vec{x}) = 1 + \sum_{i=1}^{i=n} 2^{(i-1)} x_i$ и $F_i(\vec{x}) = x_i^2 - x_i$. Тогда минимальный размер доказательства для такой системы в $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$ строго больше чем $C \cdot 2^{\frac{n}{2}}$ для некоторой константы $C > 0$.

**Доказательство.** Предположим, что минимальный размер доказательства нашей системы равенств имеет размер $p(n)$. Тогда докажем, что это опровержение можно преобразовать в $\mathbb{Z}$-опровержение, в котором константа в конце будет не больше, чем $2^{(p(n)^2)}$, так как суммарное количество битов, необходимых для записи всех знаменателей, не превосходит $p(n)$. Для этого рассмотрим все переменные $y_1, \ldots, y_k$, участвующие в нашем доказательстве. Для каждого $y_i$ нам дано равенство $y_i - Q_i(x) = 0$. Путь $M_i$ — произведение знаменателей всех коэффициентов в полиноме $Q_i(x)$. Мы знаем, что размер доказательства не больше чем $p(n)$, поэтому $M_i < 2^{p(n)}$. Теперь рассмотрим переменные $y_i = M_i y_i'$. Теперь, имея доказательство в $PC_{\mathbb{Q}}$ для системы полиномов $\{G, F_1, \ldots, F_n, y_1 - Q_1, \ldots, y_k - Q_k\}$ мы построим доказательство в системе $PC_{\mathbb{Z}}$ для системы $\{G, F_1, \ldots, F_n, y_1' - M_1 Q_1, \ldots, y_k' - M_k Q_k\}$. Пусть наше доказательство было последовательностью полиномов $R_1, \ldots, R_s$. Будем последовательно рассматривать первые $t$ полиномов в нашем выводе и на каждом шагу дописывать в конец нашего $PC_{\mathbb{Z}}$-доказательства $t$ новых полиномов.

Пусть мы уже преобразовали полиномы $R_1, \ldots, R_t$ и построили полиномы $R_1', \ldots, R_f'$ такие, что $R_1', \ldots, R_f'$ образуют корректный вывод в системе $PC_{\mathbb{Z}}$ и при этом каждый из $R'_{f-t+i}$ равен $R_i \cdot C$ для $i \leq t$ (если заменить все $y_i'$ на $M_i \cdot y_i$), где $C$ — некоторая целая константа. Тогда построим последовательность полиномов $R'_{f+1}, \ldots R'_{f+t+1}$ такую, что $R_1', \ldots, R'_{f+t+1}$ образуют корректный вывод в $PC_{\mathbb{Z}}$ и при этом $R'_{f+i}$ равен $R_i \cdot C'$ для любого $i \leq t+1$ и для некоторой новой константы $C'$. Разберем несколько случаев:

1. Если $R_{t+1} = G$ или $R_{t+1} = F$ , то

   $$R'_{f+1} = R'_{f-t+1}, \quad R'_{f+2} = R'_{f-t+2}, \quad \ldots, \quad R'_{f+t} = R'_f, \quad R'_{f+t+1} = R_{t+1} \cdot C.$$

   То есть в этом случае $C' = C$.

2. Если $R_{t+1} = y_i - Q_i$, то

   $$R'_{f+1} = M_i \cdot R'_{f-t+1}, \quad R'_{f+2} = M_i \cdot R'_{f-t+2}, \quad \ldots, \quad R'_{f+t} = M_i \cdot R'_f,$$

   а $R'_{f+t+1} = C \cdot y_i' - M_i \cdot C \cdot Q_i$, что равно $C \cdot M_i \cdot R_{t+1}$. При этом новая константа $C' = C \cdot M_i$.

3. Если $R_{t+1} = \alpha R_j + \beta R_i$, где $\alpha = \frac{p_1}{q_1}$, а $\beta = \frac{p_2}{q_2}$, то

   $$R'_{f+1} = q_1 \cdot q_2 \cdot R'_{f-t+1}, \quad R'_{f+2} = q_1 \cdot q_2 \cdot R'_{f-t+2}, \quad \ldots, \quad R'_{f+t} = q_1 \cdot q_2 \cdot R'_f,$$

   а $R'_{f+t+1} = p_1 q_2 R'_{f-t+j} + p_2 q_1 R'_{f-t+i}$. В этом случае $C' = q_1 \cdot q_2 \cdot C$.

4. Если $R_{t+1} = x_i R_j$, то

   $$R'_{f+1} = R'_{f-t+1}, \quad R'_{f+2} = R'_{f-t+2}, \quad \ldots, \quad R'_{f+t} = R'_f, \quad R'_{f+t+1} = x_i R'_{f+j}.$$

   То есть в этом случае $C' = C$.

5. Если $R_{t+1} = y_i R_j$, то

   $$R'_{f+1} = M_i R'_{f-t+1}, \quad R'_{f+2} = M_i R'_{f-t+2}, \quad \ldots, \quad R'_{f+t} = M_i R'_f.$$

   Тогда $R'_{f+t+1} = y_i' R'_{f-t+j}$. Значит $C' = C \cdot M_i$.

В результате мы получим доказательство в системе $PC_{\mathbb{Z}}$, где в конце вместо 1 получилась та самая константа $C$, которая была нашим множителем на последнем шаге построения. Но заметим, что всего у нас не более чем $p(n)$ шагов, а на каждом шагу $C$ умножается не более чем на $2^{p(n)}$. Значит $|C| < 2^{p(n)^2}$. Но по утверждению выше $|C| > 2^{exp(n)}$. Получили противоречие. □

### 3.3 Моделирование $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Q}})$ с небольшими коэффициентами

В этой секции мы промоделируем систему $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Q}})$ в системе $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$. Сразу отметим, что из нашего моделирования не будет следовать тот факт, что для любого доказательства размера $S$ в системе $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Q}})$ существует доказательство размера $poly(S)$ в системе $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$ для той же формулы. Но при этом нашего моделирования будет достаточно, чтобы доказать полиномиальную верхнюю оценку на размер доказательства формулы $\mathsf{PHP}^{n+1}_{n}$ (определение будет в следующей секции) в системе $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$. Из этого будет следовать, что система $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$ строго сильнее чем система $\mathsf{PC}$.

**Замечание.** На первый взгляд кажется, что для того чтобы полиномиально промоделировать систему $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Q}})$ в системе $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$ достаточно заменить каждую дизъюнкцию вида

$$(f_1 = 0) \vee \ldots \vee (f_m = 0),$$

появляющуюся в ходе вывода в $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Q}})$, на равенство вида $\prod f_i = 0$ в системе $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$. Именно такое моделирование было представлено в статье в статье Р. Раза, И. Цамерета [12]. В данной конструкции были промоделированы все правила вывода кроме правила сокращения одинаковых слагаемых. Проблема заключается в том, что данную операцию не получится промоделировать при помощи доказательства полиномиального размера, если коэффициенты в линейных равенствах могут иметь экспоненциальный размер. В случае, когда все коэффициенты имеют полиномиальный размер, мы покажем, что промоделировать сокращение одинаковых слагаемых можно при помощи доказательства полиномиального размера.

**Утверждение.** В системе $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Q}})$ мы можем за один шаг вывести из дизъюнкции $(1 + 2x_1 + \ldots 2^n x_n = 0) \vee (1 + 2x_1 + \ldots 2^n x_n = 0)$ равенство $(1 + 2x_1 + \ldots 2^n x_n = 0)$. Но для того, чтобы вывести в системе $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$ из $(1 + 2x_1 + \ldots 2^n x_n)^2 = 0$ равенство $(1 + 2x_1 + \ldots 2^n x_n) = 0$, нам потребуется доказательство экспоненциального размера от $n$.

**Доказательство.** Доказательство этого факта в точности повторяет нижнюю оценку для $\mathsf{BVP}_n$. А именно, нужно рассмотреть систему доказательств $\mathsf{Ext\text{-}PCR}_{\mathbb{Z}}$ и корректный вывод, начинающийся с $(1 + 2x_1 + \ldots 2^n x_n)^2 = 0$, а заканчивающийся $M \cdot (1 + 2x_1 + \ldots 2^n x_n) = 0$ для некоторой целой константы $M \neq 0$. Тогда окажется, что $M$ содержит $C \cdot 2^n$ битов. Дальше нужно доказать, что если в системе $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$ есть вывод размера $p(n)$ из равенства $(1+2x_1+\ldots 2^n x_n)^2 = 0$ равенства $(1 + 2x_1 + \ldots 2^n x_n) = 0$ , то существует вывод в системе $\mathsf{Ext\text{-}PCR}_{\mathbb{Z}}$ , начинающийся с $(1 + 2x_1 + \ldots 2^n x_n)^2 = 0$, а заканчивающийся $M \cdot (1 + 2x_1 + \ldots 2^n x_n) = 0$, где $M = O\left(2^{(p(n)^2)}\right)$. Этого будет достаточно для доказательства экспоненциальной нижней оценки.

Для того, чтобы промоделировать систему $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Q}})$, нам потребуется следующая техническая лемма:

**Лемма.** Пусть нам даны равенства вида

$$x_0 = x, x_1 = x - 1, x_2 = x - 2, \ldots, x_a = x - a,$$

$$y_0 = y, y_1 = y - 1, y_2 = y - 2, \ldots, y_b = y - b,$$

$$x_0 \cdot x_1 \cdots x_a = 0,$$
$$y_0 \cdot y_1 \cdots y_b = 0.$$

Тогда в системе $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$ из этих равенств можно вывести систему равенств

$$z_0 = x + y, z_1 = x + y - 1, z_2 = x + y - 2, \ldots, z_{a+b} = x + y - a - b,$$
$$z_0 \cdot z_1 \cdots z_{a+b} = 0$$

при помощи вывода размера $poly(ab)$.

**Доказательство.** Сначала для любого $j \in \{0, \ldots, b\}$ выведем равенство вида:

$$z_0 \cdot z_1 \cdots z_{a+b} \cdot y_0 \cdots y_{j-1} \cdot y_{j+1} \cdot y_b = 0 \tag{1}$$

Это делается следующим образом: сначала заметим, что для любых $i \in \{0, \ldots, a\}, j \in \{0, \ldots, b\}$ мы можем вывести равенство

$$z_{j+i} \cdot y_1 \cdots y_{j-1} \cdot y_{j+1} \cdot y_b = x_i \cdot y_1 \cdots y_{j-1} \cdot y_{j+1} \cdot y_b \tag{2}$$

Действительно, легко можно вывести равенство $z_{j+i} = x_i + y_j$, поэтому

$$z_{j+i} \cdot y_1 \cdots y_{j-1} \cdot y_{j+1} \cdot y_b = (x_i + y_j) \cdot y_1 \cdots y_{j-1} \cdot y_{j+1} \cdot y_b = x_i \cdot y_1 \cdots y_{j-1} \cdot y_{j+1} \cdot y_b$$

Воспользовавшись равенством $y_0 \cdot y_1 \cdots y_b = 0$ получаем равенство (2).

Тогда, применив последовательно равенство (2) для всех $i \in \{0, \ldots, a\}$, мы получим равенство

$$z_j \cdot z_{j+1} \cdots z_{j+a} \cdot y_0 \cdots y_{j-1} \cdot y_{j+1} \cdot y_b = x_0 \cdot x_1 \cdots x_a \cdot y_0 \cdots y_{j-1} \cdot y_{j+1} \cdot y_b,$$

из которого, применив равенство $x_0 \cdot x_1 \cdots x_a = 0$, получаем равенство

$$z_j \cdot z_{j+1} \cdots z_{j+a} \cdot y_0 \cdots y_{j-1} \cdot y_{j+1} \cdot y_b = 0$$

Из которого уже получаем равенство (1) домножением на недостающие переменные.

Теперь выведем равенство $z_0 \cdot z_1 \cdots z_{a+b}$. По очереди выведем все равенства вида $z_0 \cdot z_1 \cdots z_{a+b} \cdot y_0 \cdot y_1 \cdots y_k = 0$, где $k \in \{0, \ldots, b\}$.

Равенство $z_0 \cdot z_1 \cdots z_{a+b} \cdot y_0 \cdot y_1 \cdots y_{b-1} = 0$ нам дано сразу. Пусть мы уже вывели

$$z_0 \cdot z_1 \cdots z_{a+b} \cdot y_0 \cdot y_1 \cdots y_{j+1} = 0. \tag{3}$$

Мы ранее уже вывели равенство

$$z_0 \cdot z_1 \cdots z_{a+b} \cdot y_0 \cdot y_1 \cdots y_j \cdot y_{j+2} \cdots y_b = 0.$$

Имея равенства вида $y_{j+i} = y_{j+1} + i - 1$ для $i \in \{2, \ldots b - i\}$, мы можем вывести равенство

$$z_0 \cdot z_1 \cdots z_{a+b} \cdot y_0 \cdot y_1 \cdots y_j \cdot P(y_{j+1}) = 0$$

где $P(y_{j+1})$ — полином степени $b - j - 1$, в котором все коэффициенты содержат не более чем $poly(b)$ битов и свободный член равен $(-1)^{b-j-1}(b-j-1)!$. Тогда мы можем, используя равенство (3), сократив все мономы $P(y_{j+1})$ степени выше первой, вывести равенство

$$z_0 \cdot z_1 \cdots z_{a+b} \cdot y_0 \cdot y_1 \cdots y_j((-1)^{b-j-1}(b-j-1)!) = 0.$$

Сокращая константу, получаем

$$z_0 \cdot z_1 \cdots z_{a+b} \cdot y_0 \cdot y_1 \cdots y_j = 0$$

Повторив процедуру $b$ раз, получаем искомое равенство

$$z_0 \cdot z_1 \cdots z_{a+b} = 0$$

**Теорема 5.** Пусть некоторая формула в $k$-КНФ имеет опровержение размера $S$ в системе $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Q}})$, причем все константы, участвующие в этом опровержении — целые. Тогда у этой формулы существует опровержение размера $poly(max(S, M))$ в системе $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$, где $M$ — максимальная абсолютная величина целых констант, появляющихся в нашем доказательстве.

**Доказательство.** Пусть опровержение в системе $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Q}})$ имеет вид $R_1, \ldots, R_k$, где каждая строчка $R_k$ является дизъюнкцией линейных равенств. Тогда будем переписывать наше доказательство по одной строчке. Для начала, рассмотрим все линейные равенства вида $(\sum_{i=1}^{n} a_i x_i + b = 0)$, появляющиеся в дизъюнкциях $R_1, \ldots, R_k$.

Для каждой строчки $R_t$ вида $(\sum_{i=1}^{n} a_{1i} x_i + b_1 = 0) \vee \ldots \vee (\sum_{i=1}^{n} a_{ji} x_i + b_j = 0)$ мы введем новые переменные $y_{a_{11},\ldots,a_{1n},b_1}$, …, $y_{a_{j1},\ldots,a_{jn},b_j}$, для которых зададим равенства вида

$$y_{a_{11},\ldots,a_{1n},b_1} = \sum_{i=1}^{n} a_{1i} x_i + b_1, \ldots, y_{a_{j1},\ldots,a_{jn},b_j} = \sum_{i=1}^{n} a_{ji} x_i + b_j$$

Далее мы выведем для этих переменных равенство вида $y_{a_{11},\ldots,a_{1n},b_1} \cdots y_{a_{j1},\ldots,a_{jn},b_j} = 0$ и перейдем к следующей строчке. В конце мы получим равенство вида $1 = 0$ которое будет переведено в такое же равенство вида $1 = 0$, что и даст нам искомое противоречие.

Теперь формализуем написанное выше. Пусть для строчек

$$R_1 = ((f_{11} = 0) \vee \ldots \vee (f_{1p_1} = 0)), R_2 = ((f_{21} = 0) \vee \ldots \vee (f_{2p_2} = 0)), \ldots, R_t = ((f_{t1} = 0) \vee \ldots \vee (f_{tp_t} = 0))$$

мы уже ввели новые переменные $y_{f_{11}} = f_{11}, \ldots, y_{f_{tp_t}} = f_{tp_t}$ и доказали в системе $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$ равенства вида

$$y_{f_{11}} \cdots y_{f_{1p_1}} = 0, \ldots, y_{f_{t1}} \cdots y_{f_{tp_t}} = 0.$$

Рассмотрим переменную $R_{t+1}$. Посмотрим, как строчка $R_{t+1}$ могла быть выведена:

1. $R_{t+1}$ могла быть выведена при помощи правила резолюции. Это значит, что существуют $j, l < t + 1$ такие, что

   $$R_j = \big((f_{j1} = 0) \vee \ldots \vee (f_{jp_j} = 0)\big), \quad R_l = \big((f_{l1} = 0) \vee \ldots \vee (f_{lp_l} = 0)\big),$$

   $$R_{t+1} = \big((f_{j2} = 0) \vee \ldots \vee (f_{jp_j} = 0) \vee (f_{l2} = 0) \vee \ldots \vee (f_{lp_l} = 0) \vee (\alpha f_{j1} + \beta f_{l1} = 0)\big)$$

   Тогда мы знаем, что в нашем $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$ доказательстве уже выведены равенства $y_{f_{j1}} \cdots y_{f_{jp_j}} = 0$ и $y_{f_{l1}} \cdots y_{f_{lp_l}} = 0$. Тогда домножим первое равенство на $y_{f_{l2}} \cdots y_{f_{lp_l}}$, а второе на $y_{f_{j2}} \cdots y_{f_{jp_j}}$. В результате получим 2 равенства

   $$y_{f_{j1}} \cdots y_{f_{jp_j}} \cdot y_{f_{l2}} \cdots y_{f_{lp_l}} = 0 \quad \text{и} \quad y_{f_{j2}} \cdots y_{f_{jp_j}} \cdot y_{f_{l1}} \cdots y_{f_{lp_l}} = 0.$$

   Теперь введем новую переменную $y_{\alpha f_{j1} + \beta f_{l1}} = \alpha f_{j1} + \beta f_{l1}$. Сразу можем вывести, что

   $$y_{\alpha f_{j1} + \beta f_{l1}} = \alpha y_{f_{j1}} + \beta y_{f_{l1}}.$$

   Тогда сложив верхние 2 произведения с коэффициентами $\alpha$ и $\beta$ получим равенство

   $$y_{f_{j2}} \cdots y_{f_{jp_j}} \cdot y_{f_{l2}} \cdots y_{f_{lp_l}} \cdot y_{\alpha f_{j1} + \beta f_{l1}} = 0,$$

   чего мы изначально и добивались.

2. $R_{t+1}$ могла быть одной из аксиом. Тогда в качестве соответствующей ей строчки подойдет запись аксиомы в форме $\mathsf{PCR}$, а именно, если $R_{t+1} = (l_1 = 0) \vee \ldots \vee (l_t = 0)$, то в системе $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$ запись этой аксиомы будет иметь вид $l_1 \ldots l_t = 0$, где $l_i$ — переменные.

3. $R_{t+1}$ могла быть получена сокращением равенства вида $k = 0$. Тогда и в соответствующем произведении можно сократить переменную $y$, тождественно равную $k$.

4. $R_{t+1}$ могла быть выведена из $R_j$ удалением повторяющегося линейного равенства. То есть

$$R_j = \left((f_{j1} = 0) \vee (f_{j1} = 0) \vee \ldots \vee (f_{jp_j} = 0)\right),$$

$$R_{t+1} = \left((f_{j1} = 0) \vee \ldots \vee (f_{jp_j} = 0)\right).$$

Тогда мы уже вывели равенство вида

$$y_{f_{j1}} \cdot y_{f_{j1}} \cdot y_{f_{j2}} \cdots y_{f_{jp_j}} = 0.$$

По лемме мы можем вывести (так как мы знаем, что все коэффициенты линейных равенств целые), что

$$(y_{f_{j1}} + M \cdot n) \cdots (y_{f_{j1}} + 1) y_{f_{j1}} (y_{f_{j1}} - 1) \cdots (y_{f_{j1}} - M \cdot n) = 0$$

То есть мы знаем, что $P(y_{f_{j1}}) = 0$ для некоторого полинома $P$ без свободного члена и с коэффициентом перед $y_{f_{j1}}$ равным $M' \in \mathbb{Z} \backslash \{0\}$. При этом степень $P$ не выше $2M \cdot n + 1$, а коэффициенты содержат не более $poly(M \cdot n)$ бит. Тогда из равенства $y_{f_{j1}} \cdot y_{f_{j1}} \cdot y_{f_{j2}} \cdots y_{f_{jp_j}} = 0$, так как в полиноме $(P(y_{f_{j1}}) - M' \cdot y_{f_{j1}})$ нет мономов степени ниже 2, мы можем вывести равенство вида

$$(P(y_{f_{j1}}) - M' \cdot y_{f_{j1}}) \cdot y_{f_{j2}} \cdots y_{f_{jp_j}} = 0,$$

А из этого равенства, используя факт, что $P(y_{f_{j1}}) = 0$, выводим

$$M' \cdot y_{f_{j1}} \cdot y_{f_{j2}} \cdots y_{f_{jp_j}} = 0.$$

Сокращаем $M'$ и получаем требуемое равенство.

Таким образом, мы перестроили наше доказательство в доказательство в системе $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$. Заметим, что мы добавили не более чем $poly(S)$ новых переменных и при этом все константы, участвующие в новом доказательстве, не превосходят $2^{poly(T \cdot S)}$. Значит размер полученного доказательства в системе $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$ равен $poly(max(S, T))$ чего мы и добивались.

### 3.4 Следствия (верхние оценки)

**Определение.** Определим формулу $\mathsf{PHP}^{n+1}_n$. Она состоит из следующих аксиом:

**pigeon axioms:**

$$f^i = \bigvee_{j \in \{1,\ldots,n\}} x_{i,j} \quad \text{для всех } i \in \{1, \ldots, n+1\}.$$

**hole axioms:**

$$f^{i,i'}_j = (\overline{x}_{i,j} \vee \overline{x}_{i',j}) \quad \text{для всех } i \neq i' \in \{1, \ldots, n+1\}, j \in \{1, \ldots, n\}.$$

**Теорема 6.** У формулы $\mathsf{PHP}^{n+1}_n$ есть доказательство размера $poly(n)$ в системе $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$.

**Доказательство.** В статье [12] было показано, что у формулы $\mathsf{PHP}^{n+1}_n$ есть доказательство в системе $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Q}})$ в котором все константы принимают целые значения и не превосходят $poly(n)$. Значит, по теореме из секции 3.3, у этой формулы есть доказательство размера $poly(n)$ в системе $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$.

**Определение.** Определим Цейтинские формулы для данного графа $G$. Пусть дан некоторый граф $G = ([n], E)$ и некоторая функция $f : [n] \to \{0, 1\}$, задающая каждой вершине значения 0 или 1. Предположим, что $\sum_{i\in[n]} f(i) = 1$ в поле $F_2$. Тогда следующая система булевых равенств не имеет решения:

$$\bigoplus_{j:\{i,j\}\in E} x_{ij} = f(i) \quad \textbf{для всех } i \in [n]$$

Такие системы булевых равенств обычно обозначаются $\mathsf{TS}_{\mathsf{G,f}}$.

**Теорема 7.** Для любого графа $G$ на $n$ вершинах в системе Ext-PCR$_{\mathbb{Q}}$ имеется доказательство размера $poly(n)$ для формулы $\mathsf{TS}_{\mathsf{G,f}}$.

**Доказательство.** В статье [13] приводится короткое доказательство $\mathsf{TS}_{\mathsf{G,f}}$ в системе PC над базисом $\{-1, 1\}$, которая очевидно моделируется в системе Ext-PCR$_{\mathbb{Q}}$. Значит, в Ext-PCR$_{\mathbb{Q}}$ есть доказательство размера $poly(n)$ для формулы $\mathsf{TS}_{\mathsf{G,f}}$.

# 4 Система Depth-inf-PC и ее связь с Res(Lin)

## 4.1 Определения

**Определение.** Пусть $\Gamma = \{P_1, \ldots, P_m\}$ — набор полиномов над переменными $x_1, \ldots, x_n$ в поле $\mathbb{F}$ такая, что система полиномиальных равенств $P_1 = 0, \ldots, P_m = 0$ не имеет решения. Пусть $Q_1, \ldots, Q_k$ — полиномы, такие что $Q_i \in \mathbb{F}[x_1, \ldots, x_n, y_1, \ldots, y_{i-1}]$ для любого $i \geq 1$ (при $i = 1$ полином $Q_1 \in \mathbb{F}[x_1, \ldots, x_n]$). Тогда опровержением в системе Depth-inf-PC$_{\mathbb{F}}$ мы будем называть PC$_{\mathbb{F}}$-опровержение системы $\{P_1, \ldots, P_m, y_1 - Q_1, \ldots, y_k - Q_k\}$, где $y_i$ — новые переменные. Размером Depth-inf-PC$_{\mathbb{F}}$-опровержения для набора $\Gamma = \{P_1, \ldots, P_m\}$ мы будем называть наименьший возможный размер Depth-inf-PC$_{\mathbb{F}}$-опровержения для $\{P_1, \ldots, P_m, y_1 - Q_1, \ldots, y_k - Q_k\}$ по всем наборам $Q_1, \ldots, Q_k$.

Система Depth-inf-PC является обобщением системы Ext-PCR. В то же время, система IPS является обобщением системы Depth-inf-PC. Любое доказательство в системе IPS можно переписать в доказательство в системе Depth-inf-PC, а именно, для каждого гейта схемы задать собственную переменную $y_i$. Тогда в конце доказательства получится некоторый полином $f(x_1, \ldots, x_n, y_1, \ldots, y_k)$, при подстановке в который вместо каждого $y_j$ соответствующего ему полинома от переменных $x_1, \ldots, x_n$, получится 1. Но проблема в том, что при последовательной замене каждого $y_j$ на соответствующий ему полином $Q_j$, размер доказательства может возрасти экспоненциально.

Также стоит отметить, что для системы доказательств Depth-inf-PC, в отличие от системы IPS, очевидно, что проверка доказательства занимает полиномиальное время от размера доказательства.

## 4.2 Моделирование Res(Lin$_{\mathbb{Q}}$) в Depth-inf-PC

**Замечание.** Как и в случае с системой Ext-PCR, можно доказать, что в системе Depth-inf-PC нет полиномиального вывода равенства $(1+2x_1+\ldots+2^n x_n) = 0$ из равенства $(1+2x_1+\ldots+2^n x_n)^2 = 0$. Правда в этот раз нижняя оценка на размер вывода получится условная, в предположении гипотезы Шуба-Смейла из второй секции. Доказательство полностью повторяет доказательство нижней оценки для BVP$_n$ в системе IPS$_{\mathbb{Q}}$. Поэтому Depth-inf-PC не моделирует Res(Lin$_{\mathbb{Q}}$) как систему доказательств и мы будем строить моделирование в случае, когда изначальная система дизъюнкций в системе Res(Lin) порождена булевой формулой.

В этой секции мы докажем, что система $\mathsf{Depth\text{-}inf\text{-}PC}_{\mathbb{Q}}$ полиномиально моделирует систему $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Q}})$. Для этого мы сначала докажем, что система $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Z}})$ моделирует систему $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Q}})$), а затем промоделируем систему $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Z}})$ в $\mathsf{Depth\text{-}inf\text{-}PC}_{\mathbb{Q}}$.

**Теорема 8.** Пусть некоторая формула в КНФ имеет опровержение размера $S$ в системе $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Q}})$. Тогда у этой формулы существует опровержение размера $O(p(S))$ в системе $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Z}})$ для некоторого фиксированного полинома $p$.

**Доказательство.** Пусть опровержение в системе $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Q}})$ имеет вид $R_1, \ldots, R_k$, где каждая строчка $R_k$ является дизъюнкцией линейных равенств. Тогда будем переписывать наше доказательство по одной строчке. Для начала, рассмотрим все линейные равенства вида $(\sum_{i=1}^{n} a_i x_i + b = 0)$, появляющиеся в дизъюнкциях $R_1, \ldots, R_k$. Пусть наше доказательство было последовательностью полиномов $R_1, \ldots, R_s$. Будем последовательно рассматривать первые $t$ дизъюнкций в нашем выводе и на каждом шагу дописывать в конец нашего $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Z}})$-доказательства $t$ новых дизъюнкций.

Пусть мы уже преобразовали дизъюнкции $R_1, \ldots, R_t$ и построили дизъюнкции $R'_1, \ldots, R'_f$ такие, что $R'_1, \ldots, R'_f$ образуют корректный вывод в системе $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Z}})$ и при этом для каждой из дизъюнкций

$$R'_{f-t+i} = (g'_{f-t+i,1} = 0) \vee (g'_{f-t+i,2} = 0) \vee \ldots \vee (g'_{f-t+i,p_i} = 0)),$$

где $1 \leq i \leq t$, верно что

$$g'_{f-t+i,1} = C \cdot g_{i,1}, \quad g'_{f-t+i,2} = C \cdot g_{i,2}, \ldots, \quad g'_{f-t+i,p_i} = C \cdot g_{i,p_i},$$

где

$$R_i = (g_{i,1} = 0) \vee (g_{i,2} = 0 \vee \ldots \vee (g_{i,p_i} = 0)),$$

для всех $1 \leq i \leq t$, где $C$ — некоторая целая константа.

Тогда построим последовательность дизъюнкций $R'_{f+1}, \ldots R'_{f+t+1}$ такую, что $R'_1, \ldots, R'_{f+t+1}$ образуют корректный вывод в $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Z}})$ и при этом для каждой из этих дизъюнкций $R'_{f+i}$ выполнено индукционное предположение для некоторой константы $C$ для некоторой новой константы $C'$. Разберем несколько случаев:

1. Если $R_{t+1}$ — одна из дизюнкций нашей КНФ, то

   $$R'_{f+1} = R'_{f-t+1}, \quad R'_{f+2} = R'_{f-t+2}, \quad \ldots, \quad R'_{f+t} = R'_f, \quad R'_{f+t+1} = R_{t+1} \cdot C.$$

   То есть в этом случае $C' = C$.

2. $R_{t+1}$ могла быть выведена при помощи правила резолюции. Это значит, что существуют $j, l < t+1$ такие, что

   $$R_j = \left((g_{j,1} = 0) \vee \ldots \vee (g_{j,p_j} = 0)\right), \quad R_l = \left((g_{l,1} = 0) \vee \ldots \vee (g_{l,p_l} = 0)\right),$$

   $$R_{t+1} = \left((g_{j,2} = 0) \vee \ldots \vee (g_{j,p_j} = 0) \vee (g_{l,2} = 0) \vee \ldots \vee (g_{l,p_l} = 0) \vee (\alpha_1 g_{j,1} + \alpha_2 g_{l,1} = 0)\right),$$

   где $\alpha_1 = \frac{\beta_1}{\gamma_1}$, а $\alpha_2 = \frac{\beta_2}{\gamma_2}$.

   Тогда

   $$R'_{f+1} = (g'_{f-t+1,1} \cdot \gamma_1 \cdot \gamma_2 = 0) \vee \ldots \vee (g'_{f-t+1,p_1} \cdot \gamma_1 \cdot \gamma_2 = 0)),$$
   $$R'_{f+2} = (g'_{f-t+2,1} \cdot \gamma_1 \cdot \gamma_2 = 0) \vee \ldots \vee (g'_{f-t+2,p_2} \cdot \gamma_1 \cdot \gamma_2 = 0)), \quad \ldots,$$
   $$R'_{f+t} = (g'_{f,1} \cdot \gamma_1 \cdot \gamma_2 = 0) \vee \ldots \vee (g'_{f,p_f} \cdot \gamma_1 \cdot \gamma_2 = 0)),$$

а

$$R'_{f+t+1} = (g'_{f-t+j,2} \cdot \gamma_1 \cdot \gamma_2 = 0) \vee \ldots \vee (g_{f-t+j,p_j} \cdot \gamma_1 \cdot \gamma_2 = 0) \vee$$
$$\vee (g_{f-t+l,2} \cdot \gamma_1 \cdot \gamma_2 = 0) \vee \ldots \vee (g_{f-t+l,p_l} \cdot \gamma_1 \cdot \gamma_2 = 0) \vee (\beta_1 \cdot \gamma_2 g_{f-t+j,1} + \beta_2 \cdot \gamma_1 g_{f-t+l,1} = 0).$$

В этом случае $C' = \gamma_1 \cdot \gamma_2 \cdot C$.

3. $R_{t+1}$ могла быть получена сокращением $(1 = 0)$ или сокращением одинаковых дизъюнктов. В обоих случаях, константа $C' = C$, новые $t$ строчек совпадают со старыми $t$ строчками, а в последней строчке просто производится сокращение.

В результате мы получим доказательство в системе $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Z}})$, где в конце вместо 1 получилась та самая константа $C$, которая была нашим множителем на последнем шаге построения. Но заметим, что всего у нас не более чем $p(S)$ шагов, а на каждом шагу $C$ умножается не более чем на $2^{p(S)}$. Значит размер получившегося доказательства равен $O(p(S))$ для некоторого полинома $p$, чего мы и добивались.

**Теорема 9.** Пусть некоторая формула в КНФ имеет опровержение размера $S$ в системе $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Z}})$. Тогда у этой формулы существует опровержение размера $O(p(S))$ в системе $\mathsf{Depth\text{-}inf\text{-}PC}_{\mathbb{Q}}$ для некоторого фиксированного полинома $p$.

**Доказательство.** Вначале опишем наше доказательство неформально. Как мы знаем, если записать каждый дизъюнкт $(f_1 = 0) \vee \ldots \vee (f_k = 0)$ в виде произведения $\prod_i f_i$, то вывод из $f_i^2 = 0$ равенства $f_i = 0$ в системе $\mathsf{Depth\text{-}inf\text{-}PC}_{\mathbb{Q}}$ может быть суперполиномиального размера, если в $f_i$ встречаются коэффициенты размера $exp(n)$. Поэтому мы не будем переписывать вывод в таком виде, а рассмотрим для каждого равенства $f = 0$, возникающего в наших дизъюнкциях, новые переменные $y_f^{(0)}, \ldots, y_f^{(T)}$, которые будут равны полиномам, значения которых будут совпадать с битами $f$ как числа при любых булевых значениях переменных $x_i$. Тогда мы заменим каждый дизъюнкт $(f_1 = 0) \vee \ldots \vee (f_k = 0)$ на $\prod_i \left(\sum_j y_{f_i}^{(j)}\right)$. Заметим, что в $\left(\sum_j y_{f_i}^{(j)}\right)$ коэффициент перед каждым $y_{f_i}^{(j)}$ равен ровно 1. Поэтому в системе $\mathsf{Depth\text{-}inf\text{-}PC}_{\mathbb{Q}}$ существует доказательство полиномиального размера для вывода из равенства $\left(\sum_j y_{f_i}^{(j)}\right)^2 = 0$ равенства $\left(\sum_j y_{f_i}^{(j)}\right) = 0$, так как все возможные значения $\left(\sum_j y_{f_i}^{(j)}\right)$ лежат в промежутке $[0, T]$. Этим мы и воспользуемся для построения нашего моделирования.

Перейдем к формализации нашего доказательства. Пусть опровержение в системе $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Z}})$ имеет вид $R_1, \ldots, R_k$, где каждая строчка $R_k$ является дизъюнкцией линейных равенств. Тогда будем переписывать наше доказательство по одной строчке. Рассмотрим все линейные равенства вида $(\sum_{i=1}^n a_i x_i + b = 0)$, появляющиеся в дизъюнкциях $R_1, \ldots, R_k$.

Для каждой строчки $R_t$ вида $(\sum_{i=1}^n a_{1i} x_i + b_1 = 0) \vee \ldots \vee (\sum_{i=1}^n a_{ji} x_i + b_j = 0)$ мы введем новые переменные $y_{a_{11},\ldots,a_{1n},b_1}$, …, $y_{a_{j1},\ldots,a_{jn},b_j}$ для которых зададим равенства вида

$$y_{a_{11},\ldots,a_{1n},b_1} = \sum_{i=1}^n a_{1i} x_i + b_1, \ldots, y_{a_{j1},\ldots,a_{jn},b_j} = \sum_{i=1}^n a_{ji} x_i + b_j$$

Далее для каждой переменной $y_f$ мы введем новые переменные $y_f^{(0)}, \ldots, y_f^{(T)}$, по сути кодирующие битовую запись переменной $y_f$. В нашем случае мы потребуем $T = p(S)$ для некоторого полинома фиксированного полинома $p$.

Давайте сначала зафиксируем свойства, которые нам потребуются от нашего битового кодирования:

1. Если $f = M$, где $M \in \mathbb{Z}$, то мы должны при помощи доказательства размера $p(T)$ выводить, что каждая переменная $y_f^{(i)}$ равна некоторой константе. Более того, если $M \neq 0$, то для некоторого $i$, $y_f^{(i)} = 1$.

2. Мы должны уметь при помощи доказательства размера $p(T)$ вывести равенство $\left(y_f^{(i)}\right)^2 = y_f^{(i)}$ для любого $\in \{0, 1, \ldots, T\}$.

3. Если для двух линейных комбинаций $f$ и $g$ мы вывели, что $y_f^{(i)} = 0$ и $y_g^{(i)} = 0$ для любого $i \in \{0, 1, \ldots, T\}$, то мы сможем при помощи доказательства размера $p(T)$ вывести равенство $y_{\alpha f+\beta g}^{(i)} = 0$ для любого $i \in \{0, 1, \ldots, T\}$ и любых целых констант $\alpha$ и $\beta$.

4. Если $f = x$ или $f = 1 - x$ для булевых переменных из изначальной формулы, то мы сможем при помощи доказательства размера $p(T)$ вывести равенство $y_f^{(0)} = f$, $y_f^{(i)} = 0$ для всех $i \in \{1, \ldots T\}$.

Предположим, что такое кодирование в системе $\mathsf{Depth\text{-}inf\text{-}PC}_{\mathbb{Q}}$ у нас есть. Тогда будем перестраивать оригинальный вывод следующим образом: для каждой строчки $R_t$ вида $(f_1 = 0) \vee (f_2 = 0) \vee \ldots \vee (f_p = 0)$ мы выведем равенство

$$(y_{f_1}^{(0)} + y_{f_1}^{(1)} + \ldots + y_{f_1}^{(T)}) \cdot (y_{f_2}^{(0)} + y_{f_2}^{(1)} + \ldots + y_{f_2}^{(T)}) \cdots (y_{f_p}^{(0)} + y_{f_p}^{(1)} + \ldots + y_{f_p}^{(T)}) = 0.$$

В результате, в конце мы получим равенство вида $(y_f^{(0)} + y_f^{(1)} + \ldots + y_f^{(T)}) = 0$, где $f = M \in \mathbb{Z}\backslash\{0\}$. А значит, по предположению о нашем кодировании, мы можем вывести равенство $C = 0$ для некоторого $C \neq 0$, что нам и требуется.

Формализуем написанное выше. Предположим, что для строчек

$$R_1 = ((f_{11} = 0) \vee \ldots \vee (f_{1p_1} = 0)), R_2 = ((f_{21} = 0) \vee \ldots \vee (f_{2p_2} = 0)), \ldots, R_t = ((f_{t1} = 0) \vee \ldots \vee (f_{tp_t} = 0))$$

мы уже вывели равенства вида

$$z_{f_{11}} \cdots z_{f_{1p_1}} = 0, \ldots, z_{f_{t1}} \cdots z_{f_{tp_t}} = 0,$$

где $z_{f_{ij}} = (y_{f_{ij}}^{(0)} + y_{f_{ij}}^{(1)} + \cdots + y_{f_{ij}}^{(T)})$ для любой пары $i \in \{1, \ldots t\}, j \in \{1, \ldots, p_i\}$. Посмотрим, как строчка $R_{t+1}$ могла быть выведена:

1. $R_{t+1}$ могла быть выведена при помощи правила резолюции. Это значит, что существуют $j, l < t + 1$ такие, что

$$R_j = \left((f_{j1} = 0) \vee \ldots \vee (f_{jp_j} = 0)\right), \quad R_l = \left((f_{l1} = 0) \vee \ldots \vee (f_{lp_l} = 0)\right),$$

$$R_{t+1} = \left((f_{j2} = 0) \vee \ldots \vee (f_{jp_j} = 0) \vee (f_{l2} = 0) \vee \ldots \vee (f_{lp_l} = 0) \vee (\alpha f_{j1} + \beta f_{l1} = 0)\right)$$

Тогда мы знаем, что в нашем $\mathsf{Depth\text{-}inf\text{-}PC}_{\mathbb{Q}}$ доказательстве уже выведены равенства $z_{f_{j1}} \cdots z_{f_{jp_j}} = 0$ и $z_{f_{l1}} \cdots z_{f_{lp_l}} = 0$. Тогда мы можем раскрыть первое равенство как

$$(y_{f_{j1}}^{(0)} + y_{f_{j1}}^{(1)} + \ldots + y_{f_{j1}}^{(T)}) \cdot z_{f_{j2}} \cdots z_{f_{jp_j}} = 0,$$

а второе как

$$(y_{f_{l1}}^{(0)} + y_{f_{l1}}^{(1)} + \ldots + y_{f_{l1}}^{(T)}) \cdot z_{f_{l2}} \cdots z_{f_{lp_l}} = 0$$

Тогда выведем из первого равенства для всех $i \in \{0, \ldots, T\}$ новые равенства вида

$$y^{(i)}_{f_{j1}} \cdot z_{f_{j2}} \cdots z_{f_{jp_j}} = 0$$

Действительно, домножим первое равенство на $y^{(i)}_{f_{j1}}$ и сократим $\left(y^{(i)}_{f_{j1}}\right)^2 - y^{(i)}_{f_{j1}}$. Получим

$$y^{(i)}_{f_{j1}} \cdot (1 + y^{(0)}_{f_{j1}} + \ldots + y^{(i-1)}_{f_{j1}} + y^{(i+1)}_{f_{j1}} + \ldots + y^{(T)}_{f_{j1}}) \cdot z_{f_{j2}} \cdots z_{f_{jp_j}} = 0,$$

Тогда введем новую переменную $h = (1 + y^{(0)}_{f_{j1}} + \ldots + y^{(i-1)}_{f_{j1}} + y^{(i+1)}_{f_{j1}} + \ldots + y^{(T)}_{f_{j1}})$. По лемме из секции 3.3, легко доказать, что

$$(h_1) \cdot (h_2) \cdots (h_T) = 0$$

Где $h_i = h - i$ для любого $i \in \{1, \ldots, T\}$. Тогда мы можем превратить этот полином в полином от переменной $h$ степени $T$ с ненулевым свободным членом $M'$. При этом все это мы можем сделать используя $p(S)$ битов. Тогда получим, что у нас есть равенство $P(h) = 0$ и равенство вида

$$y^{(i)}_{f_{j1}} \cdot h \cdot z_{f_{j2}} \cdots z_{f_{jp_j}} = 0,$$

Значит из него мы можем получить равенство вида

$$y^{(i)}_{f_{j1}} \cdot (P(h) - M') \cdot z_{f_{j2}} \cdots z_{f_{jp_j}} = 0$$

Тогда домножим $P(h)$ на $y^{(i)}_{f_{j1}} \cdot z_{f_{j2}} \cdots z_{f_{jp_j}}$ и сложим с верхним равенством. Получим равенство вида

$$M' \cdot y^{(i)}_{f_{j1}} \cdot z_{f_{j2}} \cdots z_{f_{jp_j}} = 0$$

Сократим $M'$ и получим требуемое равенство.

Таким образом, мы получили все равенства вида

$$y^{(i)}_{f_{j1}} \cdot z_{f_{j2}} \cdots z_{f_{jp_j}} = 0$$

и

$$y^{(i)}_{f_{l1}} \cdot z_{f_{l2}} \cdots z_{f_{lp_l}} = 0,$$

так как нижние равенства получаются аналогично верхним. Тогда, используя предположение 3 о нашем кодировании, мы можем, используя $p(S)$ бит, вывести равенства вида:

$$y^{(i)}_{\alpha f_{j1} + \beta f_{l1}} \cdot z_{f_{j2}} \cdots z_{f_{jp_j}} \cdot z_{f_{l2}} \cdots z_{f_{lp_l}} = 0$$

для любого $i \in \{0, \ldots, T\}$. Тогда сложим эти равенства для всех $i \in \{0, \ldots, T\}$ и получим, что

$$(y^{(0)}_{\alpha f_{j1} + \beta f_{l1}} + y^{(1)}_{\alpha f_{j1} + \beta f_{l1}} + \ldots + y^{(T)}_{\alpha f_{j1} + \beta f_{l1}}) \cdot z_{f_{j2}} \cdots z_{f_{jp_j}} \cdot z_{f_{l2}} \cdots z_{f_{lp_l}} = 0$$

Из чего сразу выведем, что

$$z_{\alpha f_{j1} + \beta f_{l1}} \cdot z_{f_{j2}} \cdots z_{f_{jp_j}} \cdot z_{f_{l2}} \cdots z_{f_{lp_l}} = 0,$$

что нам и требовалось.

2. Теперь разберем случай, ради которого нам на самом деле и нужно битовое кодирование. Мы уже воспользовались выше тем фактом, что если у числа $T$ битов, то сумма значений его битов принимает не более $T$ возможных значений. Сейчас нам придется воспользоваться этим фактом еще раз.

   Пусть $R_{t+1}$ была выведена из $R_j$ удалением повторяющегося линейного равенства. То есть

   $$R_j = ((f_{j1} = 0) \vee (f_{j1} = 0) \vee \ldots \vee (f_{jp_1} = 0)),$$

   $$R_{t+1} = ((f_{j1} = 0) \vee \ldots \vee (f_{jp_1} = 0)).$$

   Тогда мы уже вывели равенство вида

   $$z_{f_{j1}} \cdot z_{f_{j1}} \cdot z_{f_{j2}} \cdots z_{f_{jp_j}} = 0.$$

   По лемме из прошлой секции мы можем вывести, что

   $$z_{f_{j1}}(z_{f_{j1}} - 1) \ldots (z_{f_{j1}} - T) = 0$$

   То есть мы знаем, что $P(z_{f_{j1}}) = 0$ для некоторого полинома $P$ без свободного члена и с коэффициентом перед $z_{f_{j1}}$ равным $M' \in \mathbb{Z}\backslash\{0\}$. При этом степень $P$ не выше $T$, а коэффициенты содержат не более $p(T)$ бит. Тогда из равенства $z_{f_{j1}} \cdot z_{f_{j1}} \cdot z_{f_{j2}} \cdots z_{f_{jp_j}} = 0$ мы можем вывести равенство вида

   $$(P(z_{f_{j1}}) - M' \cdot z_{f_{j1}}) \cdot z_{f_{j2}} \cdots z_{f_{jp_j}} = 0,$$

   А из этого равенства, используя факт, что $P(z_{f_{j1}}) = 0$, выводим

   $$M' \cdot z_{f_{j1}} \cdot z_{f_{j2}} \cdots z_{f_{jp_j}} = 0$$

   Сокращаем $M'$ и получаем требуемое равенство.

3. $R_{t+1}$ могла быть одной из аксиом. Тогда по свойству 4 нашего кодирования, для любой формулы $f = x$ или $f = 1 - x$, где $x$ — переменная из изначальных булевых клозов, мы знаем, что

   $$z_f = y_f^{(0)} + y_f^{(1)} + \ldots + y_f^{(T)} = f$$

   Поэтому ничего переводить вообще не нужно.

4. $R_{t+1}$ могла получиться сокращением равенства вида $M = 0$. Но тогда $z_M$ также по свойству кодирования равно некоторой константе и его можно легко сократить.

Таким образом мы разобрали все случаи и доказали, что если искомое кодирование существует, то доказательство в $\mathsf{Res}(\mathsf{Lin}_{\mathbb{Z}})$ переписывается в короткое доказательство в $\mathsf{Depth\text{-}inf\text{-}PC}_{\mathbb{Q}}$.

Осталось показать, что такое кодирование существует. Этому будет посвящена следующая секция.

### 4.3 Битовое кодирование в $\mathsf{Depth\text{-}inf\text{-}PC}_{\mathbb{Q}}$

Наша цель — построить полиномы для переменных $y_f^{(0)}, \ldots, y_f^{(T)}$, которые задают кодирование для всех переменных $y_f$, появляющихся в ходе нашего доказательства. При этом мы хотим, чтобы наше кодирование удовлетворяло свойствам, описанным в предыдущей секции. Пусть максимальное значение линейных комбинаций, при условии что переменные булевы, по модулю не превосходит $M$. Тогда выберем $T$ достаточно большое, чтобы $2^T > M^2$. Далее определим несколько операций с битовыми векторами:

1. Операция $\oplus$: пусть нам даны два битовых вектора $\overline{y} = (y_0, \ldots, y_T)$ и $\overline{x} = (x_0, \ldots, x_T)$. Тогда зададим функцию булеву функцию $H : Z_2 \times Z_2 \times Z_2 \to Z_2$ такую, что $H(a, b, c) = 1$ тогда и только тогда, когда $a + b + c \leq 2$, если рассматривать биты $a$, $b$ и $c$ как целые числа. Тогда мы можем определить вектор $\overline{c}$: $c_0 = 0$, $c_{i+1} = H(x_i, y_i, c_i)$ для всех $i \in \{1, \ldots, T\}$. Теперь мы можем определить операцию сложения:

   $$\overline{y} \oplus \overline{x} = \overline{w},$$

   где каждый бит $w_i = x_i \oplus y_i \oplus c_i$, где $\oplus$ обозначает исключающее ИЛИ. При это функция $H$, как и функция XOR, записаны в форме многочленов степени не выше 3.

   Сразу заметим полезное свойство: если мы уже вывели равенства вида $y_i^2 = y_i$ и $z_i^2 = z_i$ для всех $i \in \{0, \ldots, T\}$, то мы можем вывести равенства вида $c_i^2 = c_i$, а из них и равенства вида $w_i^2 = w_i$. При этом вывод имеет размер $poly(T)$ (для каждого $c_i$ переберем 8 возможных значений переменных $x_i, y_i, c_{i-1}$, а дальше также для $w_i$ переберем 8 значений переменных $x_i, y_i, c_i$).

   Также рассмотрим следующую лемму из статьи [14] (1 ревизия, секция 7.3, лемма 21):

   **Лемма.** Пусть нам даны 3 битовых вектора $\overline{y} = (y_1, \ldots, y_T)$, $\overline{z} = (z_1, \ldots, z_T)$, $\overline{w} = (w_1, \ldots, w_T)$. Тогда в системе $\mathsf{Depth\text{-}inf\text{-}PC}_{\mathbb{Q}}$ есть доказательство размера $poly(T)$ следующего побитового равенства:

   $$(\overline{y} \oplus \overline{z}) \oplus \overline{w} = \overline{y} \oplus (\overline{z} \oplus \overline{w}).$$

2. Также введем операцию смены знака:

   $$-(y_0, \ldots, y_T) = (1 - y_0, \ldots, 1 - y_T) \oplus (1, 0, 0, \ldots, 0).$$

   Тогда нам потребуется следующая лемма из статьи [14] (1 ревизия, секция 7.3, лемма 26):

   **Лемма.** В системе $\mathsf{Depth\text{-}inf\text{-}PC}_{\mathbb{Q}}$ есть доказательство размера $poly(T)$ следующего равенства:

   $$-(\overline{x} \oplus \overline{y}) = (-\overline{x}) \oplus (-\overline{y})$$

3. Осталась операция домножения на скаляр:

   $$(2^n)(y_0, \ldots, y_T) = (0, 0, 0, \ldots, y_0, \ldots, y_{T-n})$$

   Тогда в $\mathsf{Depth\text{-}inf\text{-}PC}_{\mathbb{Q}}$ можно доказать следующие 2 равенства, используя $poly(T)$ битов:

   (a) $2^n(\overline{x} \oplus \overline{y}) = (2^n\overline{x}) \oplus (2^n\overline{y})$. Доказательство очевидно, на самом деле мы в обоих случаях просто сдвинули все биты на $n$ вправо, равенства останутся верными по определению операции $\oplus$.

   (b) $2^n(-\overline{x}) = -(2^n\overline{x})$. Для доказательства просто заметим, что в $-(2^n\overline{x}) = (1, 1, \ldots, 1, 1 - x_0, \ldots, 1 - x_{T-n}) \oplus (1, 0, \ldots, 0)$. Тогда мы можем легко доказать, что первые $n$ битов суммы будут равны 0, а carry bit $c_n = 1$, а это значит, что мы сможем доказать, что

   $$(1, 1, \ldots, 1, 1 - x_0, \ldots, 1 - x_{T-n}) \oplus (1, 0, \ldots, 0) = \\ = (0, 0, \ldots, 0, 1 - x_0, \ldots, 1 - x_{T-n}) \oplus (0, 0, \ldots, 1, 0, \ldots, 0).$$

   используя свойство $(a)$ получаем, что

   $$2^n(-\overline{x}) = (0, 0, \ldots, 0, 1 - x_0, \ldots, 1 - x_{T-n}) \oplus (0, 0, \ldots, 1, 0, \ldots, 0),$$

   то есть $2^n(-\overline{x}) = -(2^n\overline{x})$, чего мы и хотели.

Тогда, зная эту операцию домножения на скаляр, мы можем определить операцию домножения на любое число $A \in \mathbb{Z}$. Пусть $|A| = a_0 \cdot 2^0 + a_1 \cdot 2^1 + \ldots + a_T \cdot 2^T$. Тогда, если $A > 0$, то

$$A \cdot \overline{x} = \bigoplus_{a_i \neq 0} (2^i \cdot \overline{x}).$$

Если $A = 0$, то $A \cdot \overline{x} = (0, 0, \ldots, 0)$. Если $A < 0$, то

$$A \cdot \overline{x} = -(\bigoplus_{a_i \neq 0} (2^i \cdot \overline{x})).$$

После того, как мы определили 3 наших операции, давайте наконец определим, как именно будет устроенно битовое кодирование наших линейных комбинаций $y_f$. Пусть $f = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n + b$. Тогда вектор $\overline{y_f}$, соответствующий битовой записи переменной $y_f$, будет определяться так:

$$\overline{y_f} = (a_1 \cdot (x_1, 0, \ldots, 0)) \oplus (a_2 \cdot (x_2, 0, \ldots, 0)) \oplus \ldots \oplus (a_n \cdot (x_n, 0, \ldots, 0)) \oplus (b \cdot (1, 0, \ldots 0))$$

Докажем следующую лемму:

**Лемма.** Пусть нам даны 2 линейные комбинации

$$f = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n + b, g = c_1 x_1 + c_2 x_2 + \ldots + c_n x_n + d$$

Рассмотрим комбинацию $h = \alpha f + \beta g$, где $\alpha, \beta \in \mathbb{Z}$. Тогда в $\mathsf{Depth\text{-}inf\text{-}PC}_{\mathbb{Q}}$ существует доказательство размера $poly(T)$ равенства $\overline{y}_{\alpha f + \beta g} = \alpha \overline{y_f} \oplus \beta \overline{y_g}$

**Доказательство.** Распишем наши вектора по определению:

$$\overline{y_f} = (a_1 \cdot \overline{x_1}) \oplus (a_2 \cdot \overline{x_2}) \oplus \ldots \oplus (a_n \cdot \overline{x_n}) \oplus (b \cdot \overline{1})$$

$$\overline{y_g} = (c_1 \cdot \overline{x_1}) \oplus (c_2 \cdot \overline{x_2}) \oplus \ldots \oplus (c_n \cdot \overline{x_n}) \oplus (d \cdot \overline{1})$$

$$\overline{y}_{\alpha f + \beta g} = ((\alpha a_1 + \beta c_1) \cdot \overline{x_1}) \oplus ((\alpha a_2 + \beta c_2) \cdot \overline{x_2}) \oplus \ldots \oplus ((\alpha a_n + \beta c_n) \cdot \overline{x_n}) \oplus ((\alpha b + \beta d) \cdot \overline{1})$$

Тогда распишем выражение $\alpha \overline{y_f} \oplus \beta \overline{y_g}$ и применим свойства наших операций, доказанные выше:

$$\begin{aligned}
&\alpha \overline{y_f} \oplus \beta \overline{y_g} = \\
&= \alpha((a_1 \cdot \overline{x_1}) \oplus (a_2 \cdot \overline{x_2}) \oplus \ldots \oplus (a_n \cdot \overline{x_n}) \oplus (b \cdot \overline{1})) \oplus \beta((c_1 \cdot \overline{x_1}) \oplus (c_2 \cdot \overline{x_2}) \oplus \ldots \oplus (c_n \cdot \overline{x_n}) \oplus (d \cdot \overline{1})) = \\
&= ((\alpha \cdot (a_1 \cdot \overline{x_1})) \oplus (\beta \cdot (c_1 \cdot \overline{x_1}))) \oplus \ldots \oplus ((\alpha \cdot (a_n \cdot \overline{x_n})) \oplus (\beta \cdot (c_n \cdot \overline{x_n}))) \oplus ((\alpha \cdot (b \cdot \overline{1})) \oplus (\beta \cdot (d \cdot \overline{1})))
\end{aligned}$$

Это значит, что осталось доказать, что

$$(\alpha \cdot (a_1 \cdot \overline{x_1})) \oplus (\beta \cdot (c_1 \cdot \overline{x_1})) = (\alpha a_1 + \beta c_1) \cdot \overline{x_1}$$

Но давайте заметим, что для каждого бита этих равенств, с обеих сторон написаны полиномы от переменной $x_i$, при это мы знаем, что $x_i^2 = x_i$, и что значения этих полиномов совпадают при любом значении $x_i$ (так как наша битовая арифметика корректна по определению). Значит для каждого бита нам потребуется доказательство константного размера, чтобы доказать равенство аналогичному биту другой части. Таким образом, мы сможем построить доказательство размера $poly(T)$ равенства битовых векторов $\overline{y}_{\alpha f + \beta g} = \alpha \overline{y_f} \oplus \beta \overline{y_g}$. $\square$

Освежим в памяти, какие свойства нам требовались и докажем их:

1. Если $f = M$, где $M \in \mathbb{Z}$, то мы должны легко выводить, что каждая переменная $y_f^{(i)}$ равна некоторой константе. Более того, если $M \neq 0$, то для некоторого $i$, $y_f^{(i)} = 1$.

   Как можно заметить по построению, $y_f = M \cdot (1, 0, \ldots, 0)$, что действительно дает нам, что каждый бит равен константе, но хотя бы один не равен 0.

2. Мы должны уметь легко вывести равенство $\left(y_f^{(i)}\right)^2 = y_f^{(i)}$ для любого $\in \{0, 1, \ldots, T\}$.

   Выше было замечено, что это свойство будет выведено в ходе построения наших битовых векторов.

3. Если для двух линейных комбинаций $f$ и $g$ мы вывели, что $y_f^{(i)} = 0$ и $y_g^{(i)} = 0$ для любого $i \in \{0, 1, \ldots, T\}$, то мы сможем быстро вывести равенство $y_{\alpha f+\beta g}^{(i)} = 0$ для любого $i \in \{0, 1, \ldots, T\}$ и любых целых констант $\alpha$ и $\beta$.

   Выше мы доказали, что $\overline{y}_{\alpha f+\beta g} = \alpha\overline{y_f} \oplus \beta\overline{y_g}$ выводится за $poly(T)$ шагов, то есть мы можем доказать, что $\overline{y}_{\alpha f+\beta g} = \alpha\overline{0} + \beta\overline{0} = 0$, что и требуется.

4. Если $f = x$ или $f = 1 - x$ для булевых переменных из изначальной формулы, что $y_f^{(0)} = f$, $y_f^{(i)} = 0$ для всех $i \in \{1, \ldots T\}$.

   Для $f = x$ так получается по построению, а для $f = 1 - x$ по построению мы получим $T + 1$ бит $y_f^{(0)}, \ldots, y_f^{(T)}$, каждый из которых расписывается как полином от $x$, при этом мы знаем, что значения этих полиномов при значениях $x = 0, 1$ совпадают с вектором $(1 - x, 0, 0, \ldots, 0)$. Значит мы это сможем доказать последовательно для каждого бита за $poly(T)$ шагов.

Таким образом, все свойства выполнены, значит моделирование было корректным.

# 5 Открытые вопросы и направления дальнейшего исследования

1. Как было показано в секции 3, вывод из равенства $(1 + 2x_1 + \ldots + 2^n x_n)^2 = 0$ равенства $(1+2x_1+\ldots+2^n x_n) = 0$ требует доказательства экспоненциального размера в системе Ext-$\mathsf{PCR}_{\mathbb{Q}}$. Тогда возникает вопрос, что будет, если добавить в систему PC правило извлечения корня. Более формально, можно рассмотреть систему $\mathsf{PC}^{\surd}$.

   **Определение.** Пусть $\Gamma = \{P_1, \ldots, P_m\}$ — набор полиномов над переменными $x_1, \ldots, x_n$ в поле $\mathbb{F}$ такая, что система полиномиальных равенств $P_1 = 0, \ldots, P_m = 0$ не имеет решения. Тогда опровержением для $\Gamma$ в системе доказательств $\mathsf{PC}^{\surd}$ называется последовательность полиномов $R_1, \ldots, R_s \in \mathbb{F}[x_1, \ldots, x_n]$, где $R_s = 1$ и для любой $R_l$ получается по одному из следующих правил:

   - $R_l = P_i$ для $i \in \{1, \ldots, m\}$
   - $R_l = \alpha R_j + \beta R_k$ для $\alpha, \beta \in \mathbb{F}$, $k, j < l$
   - $R_l = x_i R_j$ где $j < l$
   - $R_l = P_j$, где $P_j \in \mathbb{F}[x_1, \ldots, x_n]$ — полином, такой что $P_j^2 = R_j$ для некоторого $j < l$.

   Схожая система $\mathcal{F}$-$\mathcal{PC}_{\surd}$ также рассматривалась в статье Д. Григорьева, Э. А. Гирша [17]. Как и для системы PC, для системы $\mathsf{PC}^{\surd}$ можно определить систему Ext-$\mathsf{PCR}_{\mathbb{Q}}^{\surd}$.

Можно показать, что любое опровержение в $\mathsf{Ext\text{-}PCR}^{\surd}_{\mathbb{Q}}$ для системы полиномиальных равенств $\mathsf{BVP}_n$ имеет экспоненциальный размер. Также можно доказать, что система $\mathsf{Ext\text{-}PCR}^{\surd}_{\mathbb{Q}}$ полиномиально моделирует систему $\mathsf{Res(Lin)}_{\mathbb{Q}}$. Кроме того, легко заметить, что в системе $\mathsf{PC}^{\surd}$ из нижних оценок на степень следуют нижние оценки на размер доказательства. Полное изложение этих результатов появится в готовящемся препринте.

Возникает вопрос, сильнее ли система $\mathsf{PC}^{\surd}$ чем обычная система $\mathsf{PC}$? Можно ли доказать в такой системе нижние оценки на степень доказательства?

2. Моделирование системы $\mathsf{Res(Lin)}$ в системе $\mathsf{Ext\text{-}PCR}_{\mathbb{Q}}$ было построено только для случая, когда коэффициенты маленькие. Можно ли промоделировать систему $\mathsf{Res(Lin)}$ в случае произвольных коэффициентов?

## Список литературы


1. Stephen A. Cook; Robert A. Reckhow. The Relative Efficiency of Propositional Proof Systems. J. Symbolic Logic Vol. 44 No. 1 (1979).
2. P. Beame, R. Impagliazzo, J. Krajícek, T. Pitassi, and P. Pudlák: Lower bounds on Hilbert's Nullstellensatz and propositional proofs, Proceedings of the London Mathematical Society, (3) 73, (1996), pp.1-26.
3. D. Grigoriev, E. A. Hirsch, Algebraic proof systems over formulas. Theoretical Computer Science 303/1: 83-102, 2003.
4. J. Grochow, T. Pitassi: Circuit Complexity, Proof Complexity and Polynomial Identity Testing. Journal of the ACM, Accepted.
5. T. Pitassi: Unsolvable Systems of Equations and Proof Complexity. *Documenta Mathematica*, Extra Volume ICM III (1998), 451-460.
6. D. Grigoriev: Linear lower bound on degrees of Positivstellensatz calculus proofs for the parity, *Theor. Comput. Sci.*, 259(1-2), (2001), pp.613-622.
7. Dima Grigoriev, Nicolai Vorobjov: Complexity of Null-and Positivstellensatz proofs. Ann. Pure Appl. Logic 113(1-3): 153-160 (2001)
8. Dima Grigoriev, Edward A. Hirsch, Dmitrii V. Pasechnik: Exponential Lower Bound for Static Semi-algebraic Proofs. ICALP 2002: 257-268
9. Edward A. Hirsch. Personal communication.
10. Edward A. Hirsch, Iddo Tzameret. Personal communication.
11. Shub, Michael; Smale, Steve (1995). On the intractability of Hilbert's Nullstellensatz and an algebraic version of "NP $\neq$ P"?. Duke Math. J. 81: 47–54
12. Raz, Ran; Tzameret, Iddo. (2007). Resolution over Linear Equations and Multilinear Proofs. Annals of Pure and Applied Logic. 155. 194-224. 10.1016/j.apal.2008.04.001.
13. Grigoriev, Dima. (1998). Tseitin's Tautologies and Lower Bounds for Nullstellensatz Proofs.
14. Russell Impagliazzo, Sasank Mouli, Toniann Pitassi: The Surprising Power of Constant Depth Algebraic Proofs. Electronic Colloquium on Computational Complexity (ECCC) 26: 24 (2019)

15. Impagliazzo, R., Pudlák, P., Sgall, J. Lower bounds for the polynomial calculus and the Grobner basis algorithm. comput. complex. 8, 127–144 (1999). https://doi.org/10.1007/s000370050024

16. S. Buss, D. Grigoriev, R. Impagliazzo and T. Pitassi, "Linear gaps between degrees for the polynomial calculus modulo distinct primes,"Proceedings. Fourteenth Annual IEEE Conference on Computational Complexity (Formerly: Structure in Complexity Theory Conference) (Cat.No.99CB36317) Atlanta, GA, USA, 1999, pp. 5-, doi: 10.1109/CCC.1999.766254.

17. D. Grigoriev, E. A. Hirsch: Algebraic proof systems over formulas. TCS 303/1: 83-102, 2003.

18. Yaroslav Alekseev, Dima Grigoriev, Edward A Hirsch, and Iddo Tzameret. Semi-algebraic proofs, IPS lower bounds and the $\tau$-conjecture: Can a natural number be negative? arXiv preprint arXiv:1911.06738, 2019. Краткая версия принята к публикации в Proceedings of STOC-2020.

19. L. Lovász, Stable sets and polynomials, Discrete Mathematics, Volume 124, Issues 1–3, 1994, Pages 137-153, ISSN 0012-365X,

20. Pudlak, Pavel. (1999). On the complexity of propositional calculus. Sets and Proofs, Invited Papers from Logic Colloquium '97. 10.1017/CBO9781107325944.010.

21. Г. С. Цейтин, "О сложности вывода в исчислении высказываний", Зап. научн. сем. ЛОМИ, 8 (1968), 234–259

22. Haken A. The intractability of resolution // Theoretical Computer Science. 1985. Vol. 39. P. 297-308.

23. Russell Impagliazzo, Sasank Mouli, and Toniann Pitassi. The surprising power of constant depth algebraic proofs. Electronic Colloquium on Computational Complexity (ECCC), 26:24, 2019.

24. Clegg M., Edmonds J., Impagliazzo R. Using the Groebner basis algorithm to find proofs of unsatisfability // Proceedings of the 28th Annual ACM Symposium on Theory of Computing, STOC'96. ACM, 1996. P. 174-183.

25. Edward A. Hirsch, Iddo Tzameret. Personal communication.